



STIC Search Report

EIC 2100

STIC Database Tracking Number: 127659

TO: Kambiz Zand
Location: 4C10
Art Unit : 2132
Tuesday, July 27, 2004

Case Serial Number: 09/607430

From: Geoffrey St. Leger
Location: EIC 2100
PK2-4B30
Phone: 308-7800

geoffrey.stleger@uspto.gov


Search Notes

Dear Examiner Zand,

Attached please find the results of your search request for application 09/607430. I searched Dialog's foreign patent files, technical databases, product announcement files and general files; along with the Internet.

Please let me know if you have any questions.

Regards,



Geoffrey St. Leger
4B30/308-7800

File 275:Gale Group Computer DB(TM) 1983-2004/Jul 26
(c) 2004 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2004/Jul 26
(c) 2004 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2004/Jul 26
(c) 2004 The Gale Group
File 16:Gale Group PROMT(R) 1990-2004/Jul 26
(c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2004/Jul 26
(c)2004 The Gale Group
File 624:McGraw-Hill Publications 1985-2004/Jul 23
(c) 2004 McGraw-Hill Co. Inc
File 15:ABI/Inform(R) 1971-2004/Jul 24
(c) 2004 ProQuest Info&Learning
File 647:CMP Computer Fulltext 1988-2004/Jul W2
(c) 2004 CMP Media, LLC
File 674:Computer News Fulltext 1989-2004/Jul W1
(c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Jul 23
(c) 2004 The Dialog Corp.
File 369:New Scientist 1994-2004/Jul W2
(c) 2004 Reed Business Information Ltd.
File 810:Business Wire 1986-1999/Feb 28
(c) 1999 Business Wire
File 813:PR Newswire 1987-1999/Apr 30
(c) 1999 PR Newswire Association Inc
File 610:Business Wire 1999-2004/Jul 24
(c) 2004 Business Wire.
File 613:PR Newswire 1999-2004/Jul 24
(c) 2004 PR Newswire Association Inc

Set	Items	Description
S1	365414	VIRUS?? OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE?? OR WOR- M?? OR (MALICIOUS OR HOSTILE OR SUSPECT) () (LOGIC OR CODE OR S- OFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ? OR DATA OR INFORMATION OR PACKET? ?)
S2	56930	ANTIVIRUS OR ANTIVIRAL
S3	67487	S1(5N) (SCAN???? OR MONITOR??? OR CHECK??? OR INTERCEPT? OR PREVENT? OR IDENTIF? OR RECOGNI????? OR REMOV??? OR DELET??? OR ELIMINAT? OR ERAS??? OR ERADICAT??? OR FILTER???)
S4	51440	(UPLOAD??? OR CHECKED()IN OR INCOMING OR NEWLY()ARRIVED OR NEW()ARRIVAL? ?) (5N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ? OR - CONTENT OR DATA OR INFORMATION)
S5	358023	DOCUMENT()CONTROL OR COLLABORATIV? OR SHARED(1W) (DOCUMENT? ? OR FILE? ?)
S6	468229	PORTAL? ?
S7	765	S2:S3(50N)S4
S8	19	S2:S3(50N)S4(50N)S5:S6
S9	12	RD (unique items)
S10	45	PORTALSHIELD
S11	8857	(UPLOADED OR CHECKED()IN OR INCOMING OR NEWLY()ARRIVED OR - NEW()ARRIVAL? ?) (5N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ?)
S12	424	S2:S3(50N)S11
S13	240	RD (unique items)
S14	176	S13 NOT PD>20000627
S15	311	S2:S3(20N)S11
S16	141	S14 AND S15
S17	251	S2:S3(10N)S11
S18	111	S17 AND S14
S19	63	S4(5N) INTERCEPT?
S20	4	S2:S3(50N)S19
S21	3	RD (unique items)
S22	5	S19(50N)S1
S23	4	RD (unique items)
S24	1	S23 NOT S21
S25	2698	S1(50N) INTERCEPT?

S26 10903 INTERCEPT??? (7N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ? OR C-
ONTENT OR DATA OR INFORMATION)
S27 67195 S1 (5N) (SCAN???? OR MONITOR??? OR CHECK??? OR PREVENT? OR I-
DENTIF? OR RECOGNI????? OR REMOV??? OR DELET??? OR ELIMINAT? -
OR ERAS??? OR ERADICAT??? OR FILTER???)
S28 195 S26(20N)S27
S29 97 RD (unique items)
S30 63 S29 NOT PD>20000627

21/9/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06378323 Supplier Number: 54762833 (THIS IS THE FULLTEXT)
Border Control: An Antivirus Gateway Guide. (Technology Information)

Carden, Philip
Network Computing, p132
May 31, 1999

ISSN: 1046-4468
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2077

TEXT:

It was March 1997 when the chickens began to die-6,800 on three farms in Hong Kong's rural New Territories. The avian virus was quickly contained, but if it had not been, the reaction around the world would have been twofold: Heightened surveillance, vaccination and treatment capabilities within each respective country, and an immediate, rapid increase in border control-keeping a new virus from entering a country is much easier than trying to contain an outbreak within.

A computer virus on the Internet can spread more quickly than a biological one in the physical world. Here, too, keeping a new virus out of the corporate network is much easier than trying to eradicate one that's already infiltrated it. Filling the role of hospitals and vaccination programs on the network are client-based antivirus packages that work to protect individual workstations; the border-control function is performed by antivirus gateways-the first line of defense against network-borne viruses.

Computer viruses fall into three basic categories: boot-sector, macro and file infector. Boot-sector viruses are spread by means of modified boot sectors on floppy disks; they launch only when a computer starts up with an infected disk in its drive. Boot-sector viruses do not travel across a network and can only be defended against by client-based antivirus software (or by eliminating floppy drives).

Macro viruses infect and spread by means of macros associated with office-automation applications. These macros usually are stored as part of a document and can be transported easily as attachments to e-mail messages.

File infectors attach to executable files-when the executable file is run, so is the virus, which then spreads by attaching itself to other executable files.

Macro viruses and file infectors can travel via a network-either as e-mail attachments or by pure file transfer. Gateway-based antivirus products aim to stop the spread of these network-transported viruses by intercepting them at the network perimeter-where the corporate network meets the Internet.

The ICSA (International Computer Security Association, www.icsa.net), an affiliate of the Gartner Group, is one of two U.S. organizations that certify antivirus products. (West Coast Labs, www.westcoast.com/checkmark, is the other.) According to the ICSA's 1998 Virus Prevalence Survey, 68 percent of virus infections can be traced to disks. However, e-mail is gaining rapidly as a source of infection-rising to 32 percent last year from 9 percent in 1996.

More important than their historical prevalence, however, is the fact that network-borne viruses (such as those attached to e-mail) can spread much more quickly than those spread by diskette. On the morning of March 26, the first incidents of the Melissa macro virus were reported in the United States. By the end of the day many sites were infected. Hundreds of thousands of employees around the world received a plethora of messages, apparently from colleagues, with the subject line beginning "Important message from..." In fact, Melissa spread so quickly that the virus easily could have been inside your network before you had a chance to update antivirus gateway software, which highlights the gateway's role of augmenting rather than replacing internal antivirus protection on servers and client workstations. Melissa served as a useful wake-up call, reminding us that the virus threat continues to evolve.

The New Hackers' Choice? Paradoxically, one reason for the development of more complex viruses may be the increasing maturity of

corporate firewall implementations. When rudimentary packet filters running on routers were the primary barriers between the corporate network and the Internet, hackers could attempt to direct access to internal information using simple port-scanning techniques. However, modern firewalls make even sophisticated hacking approaches-such as IP spoofing-technically unfeasible. As a result, hackers are relying more on techniques that involve imitating or piggy-backing legitimate traffic-tasks for which viruses and Trojan horses (similar to viruses but lacking the ability to replicate on their own) are perfectly suited.

For example, a virus might enter a network as an e-mail attachment or via an FTP download (which the firewall will allow, since e-mail and FTP are legitimate user activities). The virus, now inside the corporate network, may gather information that has immediate value (for example, competitive information) or potential value (passwords for future attacks). It can then send the information back via a "trusted" service-HTTP is one-that is allowed through the firewall. Indeed, because of the blind trust often afforded HTTP, security pros jokingly refer to it as the "Universal Firewall Tunneling Protocol."

No One Is Laughing But security vulnerability is no joke. Two very recent examples are the Caligula virus and the picture.exe Trojan horse, both of which emerged earlier this year, close on the heels of Remote Explorer. Caligula is a Microsoft Word macro virus that checks to see if PGP (Pretty Good Privacy, a public key encryption tool) is installed on the machine. If it is, the user's private key ring is sent to the FTP site of The CodeBreakers, a site for virus writers. This may not represent an immediate threat, since possessing the key ring doesn't mean the bearer has access to the keys-a passphrase is required for that. However, if the user has chosen a weak passphrase, then the private key (and protected data) certainly might be compromised.

But even strong passphrases are susceptible to the picture.exe Trojan horse, which has been propagating through e-mail spam. The e-mail items contain an executable file (it's usually called manager.exe). If executed, for example, it can look in the C:

AOL

IDB

MAIN.IDX file, which contains an America Online user's cached user name and password, and send the information (along with information on recently visited URLs) to a domain that's registered in China.

Augmenting the Firewall Clearly, the firewall itself is no longer sufficient to stand guard alone on the network perimeter. It needs to be augmented with an antivirus gateway to keep malicious code from entering the corporate network and prevent content-based attacks. The antivirus gateway reduces the corporate network's exposure to the fast-growing group of macro viruses while providing a mechanism to deploy protection rapidly against new vulnerabilities and the more sophisticated network-borne viruses foreshadowed by Melissa, Caligula and picture.exe.

An efficient antivirus strategy must be built around a solid core of client and server protection, augmented with antivirus gateways. Client protection is especially important in defending against boot-sector viruses.

The advantage that an antivirus gateway provides over client-based protection is that the gateway itself can be tightly controlled. The gateway provides virus protection at the network's most vulnerable point-its interconnection to the Internet. Because it is a dedicated device, it can be updated frequently. This lets you protect internal machines against new viruses more rapidly than if you were relying on updates to those machines' client-based protection. It provides a control point for the rapid deployment of new types of protection for new types of vulnerability.

Gateway-Specific Features Performance is a major issue for any gateway product, and antivirus software is no exception. In client-based antivirus products the key performance metric is the time needed to scan the hard drive(s). In contrast, with an antivirus gateway, the key performance metric is simply throughput-the extent to which real-time scanning of huge numbers of files affects transfer latency. For a more in-depth look at the performance of these products, see "Trend InterScan Secures Top Virus-Protection Spot," at www.networkcomputing.com/1007/1007r1.html.

Apart from the efficiency of the scanning algorithms, performance is affected by the number of files that are scanned-if a product can intelligently determine which files are unlikely to be infected (for example, nonexecutable documents with no macros), it can disregard such files, thereby improving performance. If the antivirus gateway product is integrated with a firewall, the firewall often will determine which files are passed to the antivirus gateway for additional checking. This approach reduces IP-routing complexity (fewer subnets), speeds problem resolution and simplifies failover planning if you have dual firewalls. Our Interactive Buyer's Guide charts

(www.networkcomputing.com/1011/1011buyers.html) list several vendors that provide some form of firewall integration-either with their own firewall products or with third-party firewalls. The most widely supported mechanism for integration with a third-party firewall is CVP (Content Vectoring Protocol), which is a part of Check Point Software Technologies' OPSEC (Open Platform for Secure Enterprise Connectivity) framework (www.opsec.com).

The CVP defines a client/server relationship that enables distributed firewall systems to share a common content validation server (which could be an **antivirus** gateway or other content-processing system, such as one that filters inappropriate sites). When the rule base enforced on a firewall calls for **content** validation of an **incoming file** or **file** attachment, the firewall transfers the **intercepted** file to the **antivirus** gateway for further processing. The gateway determines whether the file needs to be modified (for example, virus cleaning) and returns both the decision and the file to the firewall, which then passes or drops the file based on the response and the defined security policy.

Choosing a Solution Apart from performance and firewall integration considerations, it pays to consider those issues that apply to all antivirus solutions-virus detection and handling, online updates, centralized management, logging and alerts.

Because of the large number of viruses, it's typically impractical for a corporation to determine how thoroughly an antivirus product detects viruses. And, oddly enough, neither ICSA nor West Coast Labs appears to have certified gateway antivirus products specifically (the certified products are either for client protection or server protection). It might seem reasonable to assume that a vendor's virus detection and cleaning engine would behave similarly, whether client-, server- or gateway-based. However, this is not always the case-if yours is a highly security-sensitive network, it makes sense to conduct your own validation of virus detection and cleaning capabilities.

Apart from detection, you should also look at whether the gateway product can repair infected files in real time. The good news is that all the products listed in our Interactive Buyers' Guide provide some form of real-time cleaning. But note that several products are capable of detecting more virus types than they are able to clean.

Because e-mail attachments are often compressed, it's important that gateway antivirus products be able to detect (and preferably clean) infected files that have been squeezed.

If you are testing to validate vendor claims, you might also want to check that the product uses an iterative process that is able to detect viruses in files that have been compressed more than once. (Otherwise, a hacker might sneak in a Trojan horse-like picture.exe by double compressing a file.)

Most antivirus gateways are part of a larger antivirus suite. Management capabilities are often common to the whole suite of products, and ideally will be integrated so that a single management system can be used to configure all antivirus software in the enterprise, including client, server, messaging and gateway protection. The centralized management system should be capable of logging all important events centrally and sending a variety of alerts, including SNMP traps for integration with enterprise management systems.

Most important, however, the antivirus suite needs to support automatic updates-any virus-detection engine is only as good as its latest information. To keep up with an ever-growing list of viruses, antivirus software must be continually updated with the latest virus signatures. Updates are important for all components of the antivirus suite. But for the antivirus gateway, this update capability is critical, because the

gateway is the first choice for rapid deployment of protection against new threats. When a viral pandemic threatens, the No. 1 priority must be tightening border control.

21/3,K/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

06378323 Supplier Number: 54762833 (USE FORMAT 7 FOR FULLTEXT)
Border Control: An Antivirus Gateway Guide. (Technology Information)
Carden, Philip
Network Computing, p132
May 31, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2077

... opsec.com).
The CVP defines a client/server relationship that enables distributed firewall systems to share a common content validation server (which could be an **antivirus** gateway or other content-processing system, such as one that filters inappropriate sites). When the rule base enforced on a firewall calls for **content** validation of an **incoming file** or **file** attachment, the firewall transfers the **intercepted** file to the **antivirus** gateway for further processing. The gateway determines whether the file needs to be modified (for example, virus cleaning) and returns both the decision and the...

21/3,K/2 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

14836516 SUPPLIER NUMBER: 90118458 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Internet security for your home--high-speed broadband exposes home users to new Internet threats. (Computers & Technology).
Dickson, Michael R.
Ohio CPA Journal, 61, 3, 62(2)
July-Sept, 2002
ISSN: 0749-8284 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1547 LINE COUNT: 00124

... is too confusing for the average home user. The personal firewall products from Norton and McAfee are acceptable options when combined with the company's **virus scanning** products, although when comparing features and cost, ZoneAlarm Pro 3.0 is hard to beat.

6. Purchase and install a **virus - scanning** program. A good **virus** program not only **scans** your disk looking for **viruses**, it also **intercepts incoming** email, **scans** attachments and quarantines **files** that are suspect of containing viruses. The major players automatically update their virus definition files frequently (sometimes two or more times a week) when new **viruses** are released and **identified**. I purchase an annual subscription to Norton Anti-virus, which works well with ZoneAlarm

21/3,K/3 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

01193017 CMP ACCESSION NUMBER: NWC19990531S0026
Border Control: An Antivirus Gateway Guide
Philip Carden
NETWORK COMPUTING, 1999, n 1011, PG132
PUBLICATION DATE: 990531
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Buyer's Guide
WORD COUNT: 2032

... opsec.com).

The CVP defines a client/server relationship that enables

distributed firewall systems to share a common content validation server (which could be an **antivirus** gateway or other content-processing system, such as one that filters inappropriate sites). When the rule base enforced on a firewall calls for **content** validation of an **incoming file** or **file** attachment, the firewall transfers the **intercepted** file to the **antivirus** gateway for further processing. The gateway determines whether the file needs to be modified (for example, virus cleaning) and returns both the decision and the...

30/9/40 (Item 5 from file: 636)
DIALOG(R) File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03568929 Supplier Number: 47385210 (THIS IS THE FULLTEXT)
McAfee, Symantec Sued For Anti-Virus Patent Infringement 05/14/97
Stokell, Ian
Newsbytes, pN/A
May 14, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 396

TEXT:

CUPERTINO, CALIFORNIA, U.S.A., 1997 MAY 14 (NB) -- By Ian Stokell. One of the major concerns for users of the Internet is the possibility of a virus being accidentally downloaded when transferring data. The concern has prompted a distinct market niche for software companies to exploit. Now though, Trend Micro Inc. has sued competitors McAfee Associates [NASDAQ:MCAF] and Symantec Corp. [NASDAQ:SYMC] for alleged patent infringement.

The suit, filed in the US District Court for Northern California, revolves around, what the company says is, its "recently issued US patent on computer virus detection techniques used for data carried over the Internet, electronic-mail, and groupware."

The suit names McAfee's WebShield and GroupShield anti-virus software, and Symantec's Norton Antivirus for Internet E-mail Gateways.

Trend Micro General Counsel Robert Lowe told Newsbytes that the suit has 22 different claims in it. Said Lowe, "The broadest set of claims basically addresses when you have a server **intercepting data** being sent from one computer to a second computer, when you perform certain types of **virus scanning** processes such as separating high risk data from low risk data, and having certain types of predetermined actions that occur when a virus is detected, such as deleting it or storing it in a quarantine area."

The company wants damages and a permanent injunction "to prevent McAfee and Symantec from making, using or selling infringing products."

Continued Lowe to Newsbytes, "So (the suit) structurally covers what we would consider a 'pipeline' type of virus protection, whereas the recipient of the data is not the server -- but the server is simply sitting there monitoring the pipeline, and picking out the data that can be high risk for viruses and examining it and then doing something about it."

Other claims are specifically directed to technology used in connection with electronic mail.

The company is investigating other potential patent infringers as well. Said Lowe, "We believe that there are other companies (infringing the patent). We're doing an investigation to verify that at this point. What will do as those companies and products come to light is not clear at this time, but will be decided on a case by case basis."

He concluded: "The alternatives include suing them, adding them to this lawsuit, and negotiating royalty payments."

(19970514/Press Contact: Candace Turtle, Trend Micro Inc., 408-257-1500. Reported by Newsbytes News Network: <http://www.newsbytes.com>)

THIS IS THE FULL TEXT: COPYRIGHT 1997 Newsbytes Inc. Subscription:

Published semi-weekly. Contact Newsbytes, 406 West Olive Street, Stillwater, MN 55082-4945. Phone (612) 430-1100. FAX (612) 430-0441.

COPYRIGHT 1999 Gale Group

PUBLISHER NAME: Newsbytes News Network
COMPANY NAMES: *McAfee Associates Inc.; Symantec Corp.; Trend Micro Inc.
EVENT NAMES: *370 (Patents & copyrights)
GEOGRAPHIC NAMES: *1USA (United States)
PRODUCT NAMES: *7372530 (Disk/File Management Software)
INDUSTRY NAMES: BUSN (Any type of business); CMPT (Computers and Office Automation); TELC (Telecommunications)
NAICS CODES: 51121 (Software Publishers)
TICKER SYMBOLS: MCAF; SYMC

30/9/59 (Item 1 from file: 15)
DIALOG(R) File 15:ABI/Inform(R)

01473273 01-24261

Cleansing your computer's palate

Thompson, Amy

Security Management v4ln7 PP: 101-105 Jul 1997 ISSN: 0145-9406

JRNL CODE: SEM

DOC TYPE: Journal article LANGUAGE: English LENGTH: 4 Pages

SPECIAL FEATURE: Charts

WORD COUNT: 2080

ABSTRACT: According to the National Computer Security Association's 1997 Virus Prevalence Survey, without adequate protection against their attack, macro viruses can cost organizations more than \$13,000 per month. Virus scanning software is an integral part of providing protection. Security managers looking to purchase an antivirus product must consider several factors. Among the most important are: which files get scanned and how often, whether the scanning is transparent to the user, whether it affects performance, whether it generates a warning message and activity log, how the product is managed and updated, what platforms it supports and how much it costs. Guidelines for virus scanning are presented.

TEXT: WITHOUT ADEQUATE protection against their attack, macro viruses can cost organizations more than \$13,000 per month, according to the National Computer Security Association's (NCSA) 1997 Virus Prevalence Survey. Virus scanning software is an integral part of providing protection. Security managers looking to purchase an antivirus product must consider several factors. Among the most important are: which files get scanned and how often, whether the scanning is transparent to the user, whether it affects performance, whether it generates a warning message and activity log, how the product is managed and updated, what platforms it supports, and how much it costs.

WHAT TO SCAN. Virus scanners can either scan all files, all suspicious files, or files with particular extensions designated by the administrator. Because users cannot detect a macro virus intrusion simply by viewing the document, experts such as Chey Cobb with the NCSA recommend using a product that can scan all files, not just those that look suspicious.

RICHARD JACOBS, president of Sophos Inc., agrees. He says that macro virus detection requires the scanner to recognize something other than file extensions such as .DOS or .EXE.

WHEN TO SCAN. Most scanners can scan in real-time, periodically, or manually, and as a background function or just when executed by the user. For macro viruses, Richard Ford, a virus specialist with IBM and former editor of Virus Bulletin, recommends that the scanner scan in real-time and as a background function.

SOFTWARE MANAGEMENT. Many virus scanning products on the market today are centrally managed. That is, the system administrator can configure the server from one location to respond to a detected virus in various ways, including alerting the administrator and recipient of the infected file, isolating the infected file for later cleaning or other action, deleting the infected file, or doing nothing when the file is detected. Jacobs recommends that both the system administrator and the user be alerted if a virus is detected.

UPDATES. In addition to software management, the security manager should consider whether product updates are easily obtained and how often they are provided. Scanning programs are outdated quickly as new strains of viruses are developed; therefore, obtaining frequent virus pattern updates is critical to maintaining a secure computer environment. If the organization has many users, the security manager should also note whether the software update must be conducted manually (machine by machine) or automatically through a central computer and then distributed over the network.

Warnings. Security managers should also determine whether the software gives a virus warning message. For example, when a virus is detected the

user is alerted with a preloader message such as "WARNING! The spreadsheet you just downloaded is infected with the Laroux.B virus. Call Tech Support at ext. 123 before proceeding."

Activity logs. Some products also offer activity logs that contain information such as the date the infected file was received, the name of the file and where it originated, the destination of the file, how it was sent, and the action taken when the virus was detected.

Performance. Most virus product vendors will say that their software does not affect performance and is transparent to the user. The security manager should ask for proof, such as test results, if available, or customer references.

Platforms. Most products also have a different version for the various platforms, such as DOS, Windows 3.x, NetWare, Windows NT (v1.01), Windows 95 (v 1.0), and OS/2. The security manager should ensure that the product is sold in a format that is compatible with the company's current system.

Cost. Virus scanners can range in price depending on how many computers a company has and whether the vendor offers technical support, upgrades, updates, and other services. The security manager should inquire about any "hidden" installation or maintenance costs.

Every vendor's pricing scheme will differ, the security manager should be aware that many vendors set separate prices for the server software and the number of individual workstations. Other vendors bundle both into one price. For example, Sophos Inc. sells its SWEEP product for \$895, which includes installation on one file server regardless of the number of workstations connected to that server. Rather than charging separately per server or workstation, most vendors will also issue licenses at varying prices for large corporations.

MACRO FOCUS. Security managers should be aware that not all virus scanners can detect macro viruses—the newest and fastest growing type of malicious code. (See related story on how macro viruses work, page 107.)

Some virus experts, such as Charles P. Pfleeger, author of Security in Computing, recommend using more than one antivirus product for better protection. Combining a certified all-purpose scanner with a product that detects only macro viruses is one option. A few antivirus products do focus on macro detection. Two are ON Technology's Macro VirusTrack and SecureNet Technologies, Inc.'s, MacroBlaster.

Macro VirusTrack runs as an add-in to Word and Excel. Using Word's API (application program interface), the scanner software becomes part of Word. Unlike other scanners, this program gets rid of the extra template information and converts the virus-altered document back to a virus-free document.

Using proprietary technology, Macro VirusTrack scans all files before they are opened by either Word or Excel. When the scanner finds an infected file, it automatically removes the virus and restores the file to its original state, with no loss of data or remnants of the virus left behind. The program runs in realtime and in the background so that viruses are detected and cleaned up before they spread across the network to other documents and spreadsheets. Macro VirusTrack is sold as a network product to a minimum of ten users at \$52 per user. The price decreases as more users are added—for 100 users, the price is \$20.95 per user.

Unlike other popular products that must support device drivers to operate under different operating systems such as Windows 3.1, Windows 95, and Windows NT, this scanner can detect macro viruses across all platforms. MacroBlaster from SecureNet Technologies, Inc., installs within Word, so it also works across platforms like Windows, Windows 95, Windows NT, or Macintosh. It runs in real-time on the server or on individual workstations.

Much like Macro VirusTrack, every time a document is opened in Word, MacroBlaster checks that document. If a virus is found, it is removed before the document is allowed to open. What is different, however, is that the product does not have to be upgraded. A security feature allows administrators to authorize a macro set as unchangeable. If a document's macros are modified-either by a user or a virus-the user is notified and warned and the document stays closed until an administrator authorizes it to be opened. The search for modifications eliminates the need for product updates when new macro viruses occur.

Once the virus is detected, cleaned, and the document opened, MacroBlaster creates a log of the incident.

(Table Omitted)

Captioned as: A SOFTWARE SAMPLER INTERNET. Some antivirus products focus on the most vulnerable parts of a network: connections to the Internet, e-mail, or Web browser. For example, Sophos Inc.'s SWEEP product features a technology called InterCheck that divides the task of virus detection between a client and a server. SWEEP is installed on the server and can be scheduled to scan files stored there automatically, or at various times of the day or week, sounding an alarm if a virus is discovered.

InterCheck extends protection across the network by maintaining a list of authorized programs for every workstation and monitoring unauthorized program and disk accesses. If a user attempts to access an unknown item such as a new floppy disk, a file downloaded from the Internet, or an e-mail attachment, the InterCheck client requests a virus check from the server. The file can only be accessed from the workstation if the server verifies that the file is clean.

This program uses a checksum process to scan in real-time so that the computers do not take a performance hit. That is, once a file has been checked by the scanner and found clean, the next time it is opened, the scanner only looks to see if anything has changed, instead of rescanning the document. This takes considerably less time.

SWEEP supports Windows 95, Windows NT, DOS, Windows 3.x, NetWare, OpenVMS, OS/2, and Banyan VINES. The product is updated every month through either write-protected disks or Sophos's Web site.

Trend Micro Devices, Inc., produces InterScan VirusWall, a serverbased antivirus product that detects and eliminates viruses traveling over the Internet via e-mail at the Simple Mail Transfer Protocol (SMTP) server as well as information transfer through HTTP and FTP servers.

InterScan VirusWall checks all incoming file extensions and headers. When it detects a **file** capable of containing a virus, VirusWall **intercepts** the contents of the **file** and stores it on a temporary file on the gateway machine. It then invokes the **virus - checking** program.

E-mail attachments are opened and scanned before they enter the internal network, where they are encrypted by the various mail systems such as cc:Mail, MS Exchange, or DaVinci, which block virus scanning.

When the scanner detects known viruses, it safely isolates them at the server before they reach the workstation or threaten the LAN. The user is alerted with a customized, preloaded warning message when a virus is detected. The administrator also receives an alert that identifies the source of infected files, name of the sender, date of message, and name of virus (if known). The software allows the administrator to update patterns with one click via the Internet or by diskette.

VirusWall comes in regular and select versions. With the select version, an unknown or "unfixable" virus is uploaded directly to Trend so it can be inoculated before harming the customer's system. For twenty-five users, the product costs \$795 for the regular version and \$995 for the select version. For 500 users, the regular version is \$9,995 and the select option is

\$11,995.

WebScan, sold by McAfee Associates, Inc., provides real-time protection for Internet services, Web browsers, and e-mail. The company's Trace and Code Matrix technologies pinpoint known, generic, and even new and unknown boot, file, multipartite, stealth, mutating, polymorphic, encrypted, and macro viruses.

WebScan for Windows sells for \$40 per desktop and comes with a one-year online maintenance support agreement for an extra \$49. It is compatible with all major Web browsers, including Netscape Navigator, Internet Explorer, Mosaic, NetCruiser, and MS Internet Explorer. It also hooks to e-mail packages, including Pegasus Mail and cc:Mail and automatically scans cc:Mail attachments before the user reviews them. The product also scans files that are downloaded or attached to e-mail, including .DOCs, ZIPs, self-extracting EXEs, ARCs, and ARJs. Users are alerted when a virus is detected and instructed to delete the infected file. The administrator receives a log of the incident. WebScan is compatible with Windows 95, Windows 3.x, and Windows NT.

One concern for all antivirus vendors, according to Sophos's Jacobs, is that viruses cannot be detected within encrypted or compressed e-mail or attachments. The alternative is to decompress and isolate the files on the server, scan them there, and then distribute them to the desktop if they are clean.

OTHER RESOURCES. Evaluating product criteria can be overwhelming-especially for first-time buyers or organizations with small information security departments. But some useful resources can help. Security managers may first want to consult two well-known antivirus product testers: Virus Bulletin (VB) and the NCSA.

VB is recognized as the industry benchmark for measuring virus scanner accuracy, and the NCSA certifies virus products based on VB's In the Wild List compiled by Joe Wells of IBM.

Among the twenty-one participating products in VB's January review of DOS-based antivirus software, only Norman's Virus Control was able to detect all of the in-the-wild viruses, which include macro viruses.

In the publication's March review of NetWare antivirus software, none of the thirteen products tested caught all of the in-the-wild viruses. According to Megan Skinner, assistant editor of VB, the failure rate may be due to some vendors not submitting their product's latest version with the appropriate updates.

However, a month later when the NCSA conducted its product testing, several products had made the appropriate fixes to become certified, which means that they had to detect all the current in-the-wild macro viruses. (NCSA's list of certified antivirus products can be viewed online through Security Management Online's link to their site.) It should be noted that the NCSA only tests products from vendors that are members of its Anti-virus Product Developers Consortium.

30/3,K/1 (Item 1 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02322567 SUPPLIER NUMBER: 55465746 (USE FORMAT 7 OR 9 FOR FULL TEXT)
**NEXOR Announces the First Comprehensive Solution for Secure Electronic
Messaging and Intelligent Routing; Interceptor Offers Complete Email
Management, Security and Control. (Product Announcement)**
EDGE: Work-Group Computing Report, NA
August 16, 1999
DOCUMENT TYPE: Product Announcement LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 895 LINE COUNT: 00082

... continually checking the content of both outgoing and incoming emails. It checks the origin of all incoming messages to ensure the validity of the sender, **scans** for **viruses** and **filters** out junk emails. The email is then routed, re-directed or blocked as appropriate, improving **information** flow throughout the organization.

NEXOR **Interceptor** enables organizations to establish and maintain a complete, secure electronic communications strategy to manage and protect all critical business data contained in emails. It monitors...

30/3,K/2 (Item 2 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02306770 SUPPLIER NUMBER: 54943124 (USE FORMAT 7 OR 9 FOR FULL TEXT)
**SystemWorks gets Quarterdeck utilities. (Symantec Norton SystemWorks
utilities suite) (Brief Article) (Product Announcement)**
Government Computer News, 18, 17, 46
June 14, 1999
DOCUMENT TYPE: Brief Article Product Announcement ISSN: 0738-4300
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 138 LINE COUNT: 00015

... folders containing cookies, plugins and cache files. It can track files installed over the Internet, such as ActiveX controls.

Norton CrashGuard 4.0 claims to **intercept** application, browser and system crashes, protecting against **data** loss.

Norton Web Services **checks** every patch for **viruses** and installation issues before posting, and Norton Utilities 3.0 helps recover from Microsoft Windows and Registry problems.

SystemWorks requires at least a 66-MHz...

30/3,K/3 (Item 3 from file: 275)

DIALOG(R) File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02251916 SUPPLIER NUMBER: 53385933 (USE FORMAT 7 OR 9 FOR FULL TEXT)
E-Mail Servers Patrol Their Own. (Product Information)
Kramer, Matt
PC Week, 20(1)
Oct 26, 1998
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 841 LINE COUNT: 00072

... and Trend Micro Inc.'s ScanMail.

These third-party packages use a variety of methods to scan messages as they go through the mail system, **intercepting** them to perform a **virus scan** or **content** search, then sending messages that pass muster back into the mail system for delivery to their intended recipients.

None of the major messaging systems attempts...

30/3,K/4 (Item 4 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02168261 SUPPLIER NUMBER: 20382237 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Fighting on the Internet frontline. (anti-virus software) (Buyers Guide)
Connolly, Alison
Computer Weekly, p22(1)
Jan 29, 1998
DOCUMENT TYPE: Buyers Guide ISSN: 0010-4787 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1203 LINE COUNT: 00103

... 95 and Dos are supplied
in the one box.
Sweep and Intercheck work as
communicating processes to split
the task of virus detection between
the **file** -server and workstations.
Intercheck **intercepts** infectable
files and automatically instructs
Sweep to **scan** them for **viruses** .
The software is simple to follow
and allows you to define which files
and folders to scan as well as
scheduling actions.
The Intercheck software...

30/3,K/5 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02064181 SUPPLIER NUMBER: 19411884 (USE FORMAT 7 OR 9 FOR FULL TEXT)
McAfee, Symantec Sued For Anti-Virus Patent Infringement.
Newsbytes, pNEW05140076
May 14, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 411 LINE COUNT: 00036

... told Newsbytes that the suit has 22 different claims in it. Said
Lowe, "The broadest set of claims basically addresses when you have a
server **intercepting data** being sent from one computer to a second
computer, when you perform certain types of **virus scanning** processes
such as separating high risk data from low risk data, and having certain
types of predetermined actions that occur when a virus is detected...

30/3,K/6 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02038153 SUPPLIER NUMBER: 19049107 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Viruses: sucker bait. (avoiding computer viruses) (Technology Information)
Geier, Jim
LAN Magazine, v11, n12, p101(5)
Nov, 1996
ISSN: 1069-5621 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 3206 LINE COUNT: 00254

... Integrity Shield feature protects directories and files from
viruses by write-protecting directories and .exe and .com files. The
Integrity Shield hooks into the NetWare **file** system, **intercepts file**
open events, and allows the **Virus** Protect NLM to **scan** for known
viruses .
For workstations, you need to protect against boot and file viruses
after the workstation boots. LANDesk Virus Protect, for example, backs up
the boot area...

30/3,K/7 (Item 7 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02004608 SUPPLIER NUMBER: 18864276 (USE FORMAT 7 OR 9 FOR FULL TEXT)
User-to-User. (Question and Answer) (Column)
Rubenking, Neil J.
PC Magazine, v15, n21, p375(2)
Dec 3, 1996
DOCUMENT TYPE: Column ISSN: 0888-8507 LANGUAGE: English
RECORD TYPE: Fulltext
WORD COUNT: 1658 LINE COUNT: 00129

... on your system, you may as well copy the suspect files as described here before rebooting from a clean, write-protected floppy disk.

Only "stealth" **viruses** can be **removed** with this technique. When a **virus** of this type is resident in memory, it **intercepts** any attempt to read infected **files** from disk, substituting an image of the original, uninfected file. The purpose of this behavior is to evade detection by antivirus programs. But when you...

30/3,K/8 (Item 8 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01960395 SUPPLIER NUMBER: 18508747 (USE FORMAT 7 OR 9 FOR FULL TEXT)
VirusScan disinfects Windows NT. (McAfee Associates antivirus program)
(Software Review) (Brief Article) (Evaluation)
Bailes, Lenny
Computer Shopper, v16, n8, p627(1)
August, 1996
DOCUMENT TYPE: Brief Article Evaluation ISSN: 0886-0556
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 472 LINE COUNT: 00041

... can detect more than 5,500 known strains, including boot, file, mutating, multipartite, stealth, polymorphic, and encrypted viruses. It performed quite well on our test, **recognizing** most of the **viruses** we introduced. As an added plus, VirusScan **intercepts** Word **documents** infected with the Concept virus.

In our test, viruses contained in a number of executable files were immediately detected when we attempted to copy the...

30/3,K/9 (Item 9 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01818006 SUPPLIER NUMBER: 17121699 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Symantec Claims Cure For New Hypercard Virus.
Newsbytes, pNEW08040027
August 4, 1995
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 497 LINE COUNT: 00043

... may shutdown or lockup.

SAM versions 4.0 and 3.5 customers can immediately update against this new virus by downloading the updated virus definition **file** onto their system. Once updated, SAM **Intercept** and SAM **Virus** Clinic will detect and **eliminate** the **virus** from any infected HyperCard stacks.

However, according to Symantec, a repaired stack may not run properly, in some cases, even after the virus is eliminated...

30/3,K/10 (Item 10 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2004 The Gale Group. All rts. reserv.

01782087 SUPPLIER NUMBER: 16824235 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Computer viruses revisited. (Tech Talk)
Dragan, Rich
Computer Shopper, v15, n6, p568(2)
June, 1995
ISSN: 0886-0556 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3431 LINE COUNT: 00264

... is to restore your files' boot record from a mirrored copy.
TO CATCH A VIRUS

Unfortunately, not all viruses can be caught with the standard **scan**
-and-clean anti-**virus** model. **Virus** creators try to evade anti-virus
software programs in two ways. First, stealth viruses attempt to sidestep
detection by **intercepting** calls for disk and **data** directory reads so
that the scanning program doesn't see them. Examples of these types of
offenders are the Joshi and Whale viruses.

The most...

30/3,K/11 (Item 11 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01706709 SUPPLIER NUMBER: 16301902 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Symantec AntiVirus for Macintosh 4.0. (Software Review) (Evaluation)
Becker, Loftus E., Jr.
MacWEEK, v8, n41, p34(1)
Oct 17, 1994
DOCUMENT TYPE: Evaluation ISSN: 0892-8118 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 734 LINE COUNT: 00055

...ABSTRACT: definitions from Symantec's BBS. Users of previous versions
will find these improvements significant. The program provides
comprehensive protection even against unknown viruses through its
Intercept extension, which not only **scans** potentially infected **files**
for known **viruses**, but also keeps watch over internal changes and
external actions to detect and ward off infected applications. The newly
simplified interface lets users select their...

30/3,K/12 (Item 12 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01635986 SUPPLIER NUMBER: 14027679 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Anti-virus software. (Software Review) (Central Point's Anti-Virus 2.0,
Frisk's F-Prot Professional 2.07 and nine other anti-virus software
packages are reviewed) (Evaluation)
PC User, n214, p84(13)
June 30, 1993
DOCUMENT TYPE: Evaluation ISSN: 0263-5720 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1774 LINE COUNT: 00143

... an unusual write operation. Another simple technique restores the
date stamp after infecting a file so that users won't see the changes to
the **file**.

Some stealth **viruses intercept** DOS functions to **prevent**
programs from seeing increased file sizes and odd dates, **prevent virus**
scanners from reading the infected section of a file, and return the file
to a normal state to escape detection from integrity **checkers** or
intelligent **scanners**. **Viruses** accomplish these deceptions by
intercepting any **file** -related action call and then determining and
generating the same response a non-infected file would generate.

Self-encrypting viruses encrypt their code to escape...

...simplify the process by informing users why they flag the file.

Monitoring modules, commonly called TSRs, use three common approaches. Like a scanner, some TSRs **intercept** all executable **files** before they run and **scan** them for known **viruses**. Others **check** the integrity of the file against the validation code before executing. The third type monitors the system for virus-like behavior. Apart from requiring memory...

30/3,K/13 (Item 13 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01591301 SUPPLIER NUMBER: 13451312 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Symantec AntiVirus for Macintosh. (virus-protection software) (Software Review) (New on the Menu: Quick Clicks) (Evaluation)
Taub, Eric
MacUser, v9, n4, p91(1)
April, 1993
DOCUMENT TYPE: evaluation ISSN: 0884-0997 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
WORD COUNT: 389 LINE COUNT: 00030

Like the previous versions, SAM 3.5 consists of an application and a control panel. The application, SAM **Virus Clinic**, **scans** for and repairs **virus** -infected **files**. The control panel, SAM **Intercept**, monitors your Mac and alerts you to activities that may have been caused by a virus.

Installing SAM 3.5 is a breeze. Its new...

30/3,K/14 (Item 14 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01590052 SUPPLIER NUMBER: 13511248 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The Windows Sources catalog. (Buyers Guide)
Dennis, Kathryn
Windows Sources, v1, n3, p483(16)
April, 1993
DOCUMENT TYPE: Buyers Guide ISSN: 1065-9641 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 12338 LINE COUNT: 01057

... 408-253-9600 Fax: 408-252-4694 \$129 Requires: 384K RAM

Program designed to detect and intercept more than 1,500 PC viruses and repair **files** damaged by viruses. Includes memory-resident **virus intercept** feature to **check** applications and **files** loaded into memory. Features password protection option. Detects and destroys Michelangelo virus. Includes both Windows and DOS interfaces.

PC/DACS 2.03 for Windows
PYRAMID...

30/3,K/15 (Item 15 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01587228 SUPPLIER NUMBER: 13414780 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Vaccine: The Davidsohn Group. (Software Review) (one of 24 antivirus software packages evaluated in Keeping Up Your Guard: Antivirus Software) (Evaluation)
Pastrick, Greg
PC Magazine, v12, n5, p249(3)
March 16, 1993
DOCUMENT TYPE: Evaluation ISSN: 0888-8507 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
WORD COUNT: 629 LINE COUNT: 00050

... With the TSRs active, unauthorized program or virus-like activity pops an alert box that offers reboot or program termination actions as defaults.

Vaccine's **virus prevention** relies heavily on the interaction of the antistealth TSR, the main Vaccine TSR, and the authorized program **file** (APF) list. Initially, Vaccine **intercepts** all program activity and you build an APF by authorizing its actions from the Vaccine TSR alert box. Any questionable activity may be terminated, and...

30/3,K/16 (Item 16 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01587214 SUPPLIER NUMBER: 13414750 (USE FORMAT 7 OR 9 FOR FULL TEXT)
New wave virus busters. (new approaches to protection from computer viruses) (Keeping Up Your Guard: Antivirus Software)
Pastrick, Greg
PC Magazine, v12, n5, p212(2)
March 16, 1993
ISSN: 0888-8507 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1103 LINE COUNT: 00089

... the printer port. This is actually an electrically erasable programmable ROM (EEPROM) chip that stores bootsector and partition-table contents. While the PC-cillin software **intercepts** and **removes viruses**, the critical MBR **information** is kept safe in the virus-free Immunizer Box, ready for restoration to the hard disk should it become damaged by infection.

Multix markets a...

30/3,K/17 (Item 17 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01557075 SUPPLIER NUMBER: 14412889 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Safeguarding the enterprise network. (includes directory and related articles on the Kerberos technique and on security software products) (Overview: Security) (Cover Story) (Buyers Guide)
Powell, Dave
Networking Management, v10, n12, p16(5)
Nov, 1992
DOCUMENT TYPE: Buyers Guide ISSN: 1052-049X LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1953 LINE COUNT: 00169

... in different ways each time and thus elude signature-based scanners.

A range of networks can be protected using Symantec Corp.'s \$129 Norton Anti-**Virus** 2.0. Its 1-KB **scanner** runs continuously behind both DOS 3.1 and Windows 3.0 applications, and **intercepts** infected **files** that attempt to launch from NetWare, 3 + Open, OS/2 LAN Manager, Vines, and Starlan servers. Norton AntiVirus also offers recursive scanning, which can be...

30/3,K/18 (Item 18 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01528500 SUPPLIER NUMBER: 12288276 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Keeping viruses off net a battle.
Schneier, Bruce
MacWEEK, v6, n24, p20(2)
June 22, 1992
ISSN: 0892-8118 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1025 LINE COUNT: 00084

... Virus-Blockade can be configured to scan files immediately after they are created or modified, so if someone drops a file on your hard disk, **Virus** -Blockade will automatically **check** it for **viruses**," Shulman said.

However, running virus- **intercept** programs on **file** servers themselves can create problems. For instance, copying an infected file onto a server could bring up a dialog box that cannot be cleared remotely...

30/3,K/19 (Item 19 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01512533 SUPPLIER NUMBER: 12077360 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Virus hunting software keeps 'beasties' out. (Virus Secure from Abacus, Norton AntiVirus from Symantec Corp. and PC-cillin from Trend) (Software Review) (Desktop Directions: Virus Detection) (Evaluation)
Greiner, Lynn
Computing Canada, v18, n8, p37(1)
April 13, 1992
DOCUMENT TYPE: Evaluation ISSN: 0319-0161 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 915 LINE COUNT: 00070

... x or later. It is menu-driven and supports a mouse. Unlike Virus Secure, Norton works on Novell and IBM Token Ring networks. Its configuration **files** are password protected.

Virus **Intercept** will notify you -- loudly -- if it **recognizes** a **virus** during operation, and will automatically halt the offending program. You can customize its warning messages so, for example, network users can be told to notify...

30/3,K/20 (Item 20 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01498426 SUPPLIER NUMBER: 11928085 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Intel's LANProtect detects 850 viruses over NetWare LANs. (Intel Corp.'s LANProtect data security software, Novell Inc.'s NetWare network operating system, local area networks) (brief article) (Product Announcement)
Krohn, Nico
PC Week, v9, n7, p50(1)
Feb 17, 1992
DOCUMENT TYPE: Product Announcement ISSN: 0740-1604 LANGUAGE:
ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 384 LINE COUNT: 00030

... designed to identify 850 viruses, monitors all files sent to or from a NetWare 3.11 server. Network administrators can also configure the program to **scan** individual workstations for **viruses** without requiring that software be loaded on the client system.

The virus-detection software **intercepts** all **files** that cross network cabling on their way to or from the server, comparing them to a library of patterns that typically identify viruses, according to...

30/3,K/21 (Item 21 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01456685 SUPPLIER NUMBER: 11400315 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Data Physician Plus. (Digital Dispatch Inc.'s Data Physician Plus 1.3C) (Software Review) (one of 20 evaluations of data security software in 'On Guard: 20 Utilities That Battle the Virus Threat') (evaluation)
Fersko-Weiss, Henry

PC Magazine, v10, n18, p217

Oct 29, 1991

DOCUMENT TYPE: evaluation ISSN: 0888-8507 LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT; ABSTRACT

WORD COUNT: 534 LINE COUNT: 00041

... INTERCEPTION

The three modules with the broadest applications are Resscan, VirAlert, and VirHunt. The memory-resident Resscan monitors files, the boot sector, and memory for **viruses**. It **checks** for **virus** signatures and uses checksums and CRC checking. VirAlert, a device driver placed in the CONFIG.SYS **file**, operates continually in the background and **intercepts** attempts to manipulate executable and operating-system **files**, activity that may indicate a **virus** attack.

VirHunt is a **virus scanner** that detects and **removes** most known **viruses** and their variants. The first screen starts a search and lists all search parameters. From the second screen, you select the directory to search, specify...

30/3,K/22 (Item 22 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2004 The Gale Group. All rts. reserv.

01430074 SUPPLIER NUMBER: 10710539 (USE FORMAT 7 OR 9 FOR FULL TEXT)

SAM upgrade a shot in the arm. (Software Review) (Symantec Anti-Virus for Macintosh) (includes related summary article) (evaluation)

Costa, Steve; Antonoff, Lauren

MacWEEK, v5, n18, p42(1)

May 7, 1991

DOCUMENT TYPE: evaluation ISSN: 0892-8118 LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT; ABSTRACT

WORD COUNT: 1594 LINE COUNT: 00121

...ABSTRACT: virus detection and removal program provides a much-needed upgrade to the user interface while remaining highly configurable. The package consists of two programs: SAM **Intercept**, a **virus - scanning Startup document** (INIT), and **Virus Clinic**, a separate application that can be opened from within Intercept under System 7.0. SAM Intercept offers several levels of protection. It can notify...

... the SAM 3.0 package even though most people will not need to use it often. One advantage SAM Virus Clinic has over some other **virus - removal** programs is that -- like SAM Intercept and SAM **Intercept Jr.** -- it uses a separate **file** called SAM Virus Definitions, which can be updated to enable SAM to detect and get rid of new viruses as they are found and analyzed...

30/3,K/23 (Item 23 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)

(c) 2004 The Gale Group. All rts. reserv.

01421467 SUPPLIER NUMBER: 10440487 (USE FORMAT 7 OR 9 FOR FULL TEXT)

SAM 3.0 features on-line updating. (Symantec Corp.'s Symantec AntiVirus for Macintosh 3.0) (product announcement)

Norr, Henry

MacWEEK, v5, n10, p4(1)

March 12, 1991

DOCUMENT TYPE: product announcement ISSN: 0892-8118 LANGUAGE:

ENGLISH RECORD TYPE: FULLTEXT

WORD COUNT: 261 LINE COUNT: 00021

... to repair damage from new viruses. Updating SAM 2.0's repair function required purchasing a new disk from Symantec.

>Automatic Desktop disinfection. The SAM **Intercept Startup document** (INIT) now automatically disinfects any Desktop file contaminated with WDEF or other **viruses**.

>New **scanning** options. Users now can scan their disks from the

Control Panel without launching the SAM Virus Clinic application. Timed macros now permit after-hours scanning...

30/3,K/24 (Item 24 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01415874 SUPPLIER NUMBER: 09740887 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Norton AntiVirus battles 142 threats with three methods. (Symantec Corp.'s computer virus protection software) (Software Review) (PC Week Labs First Look) (evaluation)
Nielsen, Paul
PC Week, v8, n1, p30(2)
Jan 7, 1991
DOCUMENT TYPE: evaluation ISSN: 0740-1604 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 574 LINE COUNT: 00046

ABSTRACT: Symantec Corp's \$129.95 Norton AntiVirus data security software can **identify** 142 different computer **viruses** and provides three methods of virus protection. The program can find other **viruses** by **monitoring file** read checksums. The memory-resident **Intercept** module **monitors** disk reads for evidence of **viral** activity. The Virus Clinic module searches for viruses in memory and on disk. AntiVirus attempts to remove viruses it detects and repair virus-related damage...

... the Norton AntiVirus database, Taiwan3 is not.

Recovery from either virus required a disk reformat and new installation of Norton AntiVirus.

Although the V101 (Plastique) **virus** was detected during disk **scan** and **file** copy, Norton AntiVirus' **Intercept** feature did not alert PC Week Labs when the virus was executed. When run, V101 promptly infected the NAV.EXE file.

In a network setting...

...found "unknown" viruses on clean files. These false alarms were most likely caused by executable files that contained embedded graphic data that apparently resembled a **virus** search string.

Although Intercept **scans** disk reads for **viruses**, it does not **scan** disk writes and therefore will not uncover a virus during file decryption or uncompression.

As a kind of **file** inoculation, **Intercept** creates a checksum **file** for each executable **file** read. By watching for checksum changes, **Intercept** can warn users against undiagnosed **viruses**.

The **Virus** Clinic can **scan** entire drives or specific directories. After **scanning** its own code for **viruses**, it **scans** RAM for active or inactive **viruses** and then **checks** all executable files.

The installation is very smooth, and the product's pull-down menus are easy to use. Norton AntiVirus can be configured to...

30/3,K/25 (Item 25 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01381552 SUPPLIER NUMBER: 09436921 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Norton AntiVirus detects, intercepts DOS PC viruses. (Symantec Corp. to introduce Norton AntiVirus for DOS microcomputers) (product announcement)
Sullivan, Kristina B.
PC Week, v7, n38, p32(1)
Sept 24, 1990
DOCUMENT TYPE: product announcement ISSN: 0740-1604 LANGUAGE:
ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 304 LINE COUNT: 00024

... to be shipped next month, is designed to detect viruses in DOS PCs by examining each file loaded from a floppy disk or a network **file** server. A 17K-byte, memory-resident "**virus intercept**" feature also

checks each application and **file** that is loaded into memory, said Rod Turner, executive vice president of Symantec in Cupertino, Calif.

The Norton AntiVirus, which integrates protection, detection and eradication...

30/3,K/26 (Item 26 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01370291 SUPPLIER NUMBER: 09424823 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Finder thwarts attempts to trash virus scanner. (getting rid of the SAM icon when removing the SAM Intercept virus checker from your Mac system)

Ramsey, David

MacWEEK, v4, n30, p70(1)

Sept 11, 1990

ISSN: 0892-8118

LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT; ABSTRACT

WORD COUNT: 693 LINE COUNT: 00049

... System folder (but not into the Trash), then reboot your Mac and throw it away.

The reason the Finder wouldn't let you throw SAM **Intercept** away was that the **file** was, in fact, in use. SAM **Intercept** is a Startup **document** (INIT); after you boot, it's running all the time, **checking** disks for **viruses**. By dragging SAM out of the System folder and rebooting, you made sure that it wouldn't start running at boot time, since only the...

30/3,K/27 (Item 27 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01369464 SUPPLIER NUMBER: 08624726 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Rival, SAM: two new virus fighters leading the pack. (Software Review)

(Microseeds Publishing Inc. Rival 1.1; Symantec Antivirus for the Macintosh 2.02) (evaluation)

Westland, Mary Jane

MacWEEK, v4, n25, p62(3)

July 10, 1990

DOCUMENT TYPE: evaluation

ISSN: 0892-8118

LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT; ABSTRACT

WORD COUNT: 1309 LINE COUNT: 00102

...ABSTRACT: and files as they are opened. It is fast, transparent, and has a convenient user interface. Rival's 'Check Analysis' mode detects but does not **remove viruses**. 'Repair Analysis' **removes viruses** and can 'stun' them in files on locked volumes to prevent them from infecting other **files**. SAM 2.02 consists of an 'Intercept' cdev and a 'Virus Clinic' application. The Intercept **monitors** all activity and alerts the user to suspicious changes, while the 'Clinic' repairs infected **files** found by **Intercept**. Both companies provide excellent technical support: Microseeds updates Rival via add-in modules, while Symantec sends mailings to registered users about new viruses.

30/3,K/28 (Item 28 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01301857 SUPPLIER NUMBER: 07484492 (USE FORMAT 7 OR 9 FOR FULL TEXT)

GCC and Connect hone software. (GCC Technologies; Connect Inc) (column)

LePage, Rick,; Ford, Ric

MacWEEK, v3, n28, p18(1)

August 1, 1989

DOCUMENT TYPE: column

ISSN: 0892-8118

LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT

WORD COUNT: 649 LINE COUNT: 00052

... susceptible to the bug than Apple mice.

Shifting SAM. Symantec's Anti-Virus for the Macintosh (SAM) has proved itself a useful tool in fighting **viruses**. Its floppy- **checking** feature is a valuable one, but there are some tricks to making other software get along well with SAM **Intercept**.

Two incompatibilities with Startup **documents** (INITs) reportedly can be resolved by renaming the files so they are lower in alphabetical order than SAM and thus load first. These are SuperMac...

30/3,K/29 (Item 29 from file: 275)

DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01281203 SUPPLIER NUMBER: 07304932

SAM identifies virus-infected files, repairs applications. (Software Review) (First look) (evaluation)

Miller, Michael J.

InfoWorld, v11, n21, p61(1)

May 22, 1989

DOCUMENT TYPE: evaluation

ISSN: 0199-6649

LANGUAGE: ENGLISH

RECORD TYPE: ABSTRACT

...ABSTRACT: It advises the user of the type of virus it finds and what files have been infected. It also permits the user to repair infected **files**. **Intercept** sits above the user interface and detects a **virus** before it does damage. It **scans** floppies when they are inserted and will assist in the detection of the source of a virus. SAM sells for \$99.95.

30/3,K/30 (Item 1 from file: 621)

DIALOG(R)File 621:Gale Group New Prod. Annou. (R)
(c) 2004 The Gale Group. All rts. reserv.

02428564 Supplier Number: 60057286 (USE FORMAT 7 FOR FULLTEXT)

Trend Micro's Exchange Antivirus Software Supports New Microsoft Virus Scan API.

Business Wire, p1308

March 13, 2000

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1006

... the Beta 2 stage of product development and is scheduled to ship on March 30, 2000.

ScanMail for Exchange 3.5 features

-- Earlier detection and **elimination** of auto-executing **viruses** by

intercepting and **scanning** at the **Information**

Store before mail

hits the Exchange server mailboxes

-- Real-time scanning and blocking of both inbound and outbound messages, including previously unknown macro viruses, ensuring...

30/3,K/31 (Item 2 from file: 621)

DIALOG(R)File 621:Gale Group New Prod. Annou. (R)
(c) 2004 The Gale Group. All rts. reserv.

02230404 Supplier Number: 57528912 (USE FORMAT 7 FOR FULLTEXT)

Panda Presents New Features of Global Virus Insurance 24H-365d At Comdex Fall '99; The Latest Version Includes Protection for Lotus Notes, Improved Centralized Administration.

Business Wire, p0109

Nov 12, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 635

... S, NT Server, 3.x, DOS, OS/2, NetWare, Exchange).

Lotus Notes is a widely extended tool for groupware. Through Panda Antivirus Platinum, detection and **elimination** of **viruses** inside NSF files is fast and efficient. Detection is performed by the resident module, which allows the antivirus to **intercept**, in real-time, any infected attached **file** in replicating databases.

Panda Antivirus for Lotus Notes has been specifically developed for this system, as the only one known to protect all the databases...

30/3,K/32 (Item 3 from file: 621)

DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

(c) 2004 The Gale Group. All rts. reserv.

01655394 Supplier Number: 48490186 (USE FORMAT 7 FOR FULLTEXT)

Symantec Brings New Version of Top-Selling Macintosh Antivirus Software Into Norton Family of Products

PR Newswire, p518LAM061

May 18, 1998

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1248

... and safely.

Faster Scans in PowerPC Native Environment

Norton AntiVirus for Macintosh is now PowerPC native, which means that Norton AntiVirus Auto Protect (formerly SAM **Intercept**) **scans files** for **viruses** faster than ever. In addition, Norton AntiVirus for Macintosh is HFS+ compatible, so users can scan hard drives and disks that are using the standard...

30/3,K/33 (Item 4 from file: 621)

DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

(c) 2004 The Gale Group. All rts. reserv.

01411332 Supplier Number: 46584385 (USE FORMAT 7 FOR FULLTEXT)

Dr. Solomon's first with on-demand, on-access detection for new excel macro virus, "XM.laroux".

Business Wire, p07311209

July 31, 1996

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 463

... access protection against XM.Laroux, in the form of a detection file, consists of memory resident programs - a TSR (VirusGuard) and a VxD (WinGuard) - which **intercept** and scan any **file** before the user can access it. If the file has a **virus** then the user is **prevented** from opening it, and therefore from spreading an infection. If there is no virus, then file access continues as normal. Dr. Solomon's has this...

30/3,K/34 (Item 5 from file: 621)

DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

(c) 2004 The Gale Group. All rts. reserv.

01388764 Supplier Number: 46434963 (USE FORMAT 7 FOR FULLTEXT)

Dr. Solomon's continuously protects Windows NT users from computer viruses.

Business Wire, p6031214

June 3, 1996

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 523

(USE FORMAT 7 FOR FULLTEXT)

TEXT:

...virus scanning capability. This major enhancement automatically scans every file on access, including files on floppy disks or downloads from the Internet, in order to **intercept** computer **viruses**. It **checks** every **file** written to the Windows NT server from any attached client.

... get peace of mind and save time because they no longer have to manually scan every file or disk they access."

WinGuard for Windows NT **prevents** users from running **virus** -infected programs by **intercepting** the virus and disinfecting the original **file** before it can harm the system. WinGuard for Windows NT is a true 32-bit Windows utility. It checks the boot sectors on every floppy...

30/3,K/35 (Item 6 from file: 621)

DIALOG(R)File 621:Gale Group New Prod.Annou.(R)

(c) 2004 The Gale Group. All rts. reserv.

01320476 Supplier Number: 45936333 (USE FORMAT 7 FOR FULLTEXT)

SYMANTEC ANNOUNCES pcANYWHERE32 FOR WINDOWS 95 AND WINDOWS NT

PR Newswire, pl113SJM006

Nov 13, 1995

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1276

... increase in speed and efficiency, pcANYWHERE32 provides secure access to remote applications and data. pcANYWHERE32 includes Symantec's market-leading Norton AntiVirus technology that automatically **checks** files for **viruses** before they are transferred to a user's machine. It provides login and password protection, **data** encryption to prevent **data** from being **intercepted** during a remote session, and **file** transfer rights that can be limited by caller. Host control/audit of calls also prevents unauthorized access to the Host. Under both Windows 95 and...

30/3,K/36 (Item 1 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

(c) 2004 The Gale Group. All rts. reserv.

04429461 Supplier Number: 55745490 (USE FORMAT 7 FOR FULLTEXT)

REFLEX: New software from Reflex prevents intro of unauthorised programs and viruses from CDs.

M2 Presswire, pNA

Sept 14, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade

Word Count: 1090

... additional assurance, customers can add popular third party AV scanners of their own choice to Administrator PCs.) All Client PCs have their own dedicated macro **virus scanner**, Reflex Macro **Interceptor**, and the ability to authorise media containing **data** only.

If a PC user attempts to contravene the organisation's security

30/3,K/37 (Item 2 from file: 636)

DIALOG(R)File 636:Gale Group Newsletter DB(TM)

(c) 2004 The Gale Group. All rts. reserv.

04215097 Supplier Number: 55075886 (USE FORMAT 7 FOR FULLTEXT)

NEXOR: NEXOR Interceptor -- The next generation of secure messaging and intelligent routing technology.

M2 Presswire, pNA

July 6, 1999

Language: English Record Type: Fulltext

Document Type: Newswire; Trade
Word Count: 784

... large organisation and from the external world escalates, it is vital to supervise the flow of information in order to manage and protect business critical **data** ."

NEXOR **Interceptor** allows the definition and maintenance of a secure electronic communications strategy. It is able to **identify** junk email and information containing **viruses** before they enter the organisation and cause problems. It can also check the origins of a message, the authorisation level and the content - the email...

30/3,K/38 (Item 3 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

04111408 Supplier Number: 54042113 (USE FORMAT 7 FOR FULLTEXT)
REFLEX MAGNETICS: New macro virus can send users' personal details to notorious virus exchange site.
M2 Presswire, pNA
March 5, 1999
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1332

... to the notorious Codebreakers virus exchange (VX) site. Reflex's product development partner, Australian company Leprechaun Software International, has added modifications to its dedicated macro **virus scanner** Reflex Macro **Interceptor** (RMI) that enable it to "clean" **documents** infected by both HSFY and Ethan. A free of charge, 30-day trial version of RMI incorporating these modifications is available on request from Reflex...

30/3,K/39 (Item 4 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03725967 Supplier Number: 48052512 (USE FORMAT 7 FOR FULLTEXT)
INTEGRALIS: MIMESweeper steps up content security for Lotus Notes
M2 Presswire, pN/A
Oct 15, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 492

... MIMESweeper v3.1 is also compliant with cc:Mail release 8. MIMESweeper v3.1 runs on Windows NT 3.51 and 4.0. It will **prevent viruses** within emails or FTP and HTTP **files** from reaching users by automatically **intercepting** all inbound and outbound messages from and within a Lotus Notes server. MIMESweeper then recursively disassembles messages before undertaking content analysis. It will also help...

30/3,K/40 (Item 5 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03568929 Supplier Number: 47385210 (USE FORMAT 7 FOR FULLTEXT)
McAfee, Symantec Sued For Anti-Virus Patent Infringement 05/14/97
Stokell, Ian
Newsbytes, pN/A
May 14, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 396

... told Newsbytes that the suit has 22 different claims in it. Said Lowe, "The broadest set of claims basically addresses when you have a server **intercepting data** being sent from one computer to a second computer, when you perform certain types of **virus scanning** processes such as separating high risk data from low risk data, and having certain types of predetermined actions that occur when a virus is detected...

30/3,K/41 (Item 6 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

03213467 Supplier Number: 46591595 (USE FORMAT 7 FOR FULLTEXT)
DR.SOLOMON'S SOFTWARE: Dr. Solomon's first with detection for new excel macro virus, "XM.laroux"
M2 Presswire, pN/A
August 1, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 487

... access protection against XM.Laroux, in the form of a detection file, consists of memory resident programs - a TSR (VirusGuard) and a VxD (WinGuard) - which **intercept** and scan any **file** before the user can access it. If the file has a **virus** then the user is **prevented** from opening it, and therefore from spreading an infection. If there is no virus, then file access continues as normal. Dr. Solomon's has this...

30/3,K/42 (Item 7 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02920236 Supplier Number: 45939590 (USE FORMAT 7 FOR FULLTEXT)
SYMANTEC: Symantec announces pcANYWHERE32 for Windows 95 and Windows NT
M2 Presswire, pN/A
Nov 15, 1995
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 1294

... increase in speed and efficiency, pcANYWHERE32 provides secure access to remote applications and data. pcANYWHERE32 includes Symantec's market-leading Norton AntiVirus technology that automatically **checks** files for **viruses** before they are transferred to a user's machine. It provides login and password protection, **data** encryption to prevent **data** from being **intercepted** during a remote session, and **file** transfer rights that can be limited by caller. Host control/audit of calls also prevents unauthorized access to the Host. Under both Windows 95 and...

30/3,K/43 (Item 8 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

02817221 Supplier Number: 45713406 (USE FORMAT 7 FOR FULLTEXT)
Symantec Claims Cure For New Hypercard Virus 08/04/95
Newsbytes, pN/A
August 4, 1995
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 480

... may shutdown or lockup.
SAM versions 4.0 and 3.5 customers can immediately update against this new virus by downloading the updated virus definition **file** onto their system. Once updated, SAM **Intercept** and SAM **Virus Clinic** will detect

and **eliminate** the **virus** from any infected HyperCard stacks.

However, according to Symantec, a repaired stack may not run properly, in some cases, even after the virus is eliminated...

30/3,K/44 (Item 9 from file: 636)
DIALOG(R)File 636:Gale Group Newsletter DB(TM)
(c) 2004 The Gale Group. All rts. reserv.

01812251 Supplier Number: 43063522 (USE FORMAT 7 FOR FULLTEXT)
ANTI-VIRUS SOFTWARE: FIFTH GENERATION SYSTEMS ANNOUNCES NEW VERSIONS OF UNTOUCHABLE & UNTOUCHABLE NETWORK ANTI-VIRUS SOFTWARE
EDGE: Work-Group Computing Report, v3, n107, pN/A
June 8, 1992
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 611

... virus signatures, it provides users with an immediate solution to infection by unknown viruses.

-- Smart File Access Technology -- This allows the product to combat stealth **viruses** on-line. Stealth **viruses** **identify** the correct file size and date of an application before infection. The virus will then **intercept** operations that ask for that **information** and substitute preinfection values, not the actual values from the disk read. This effectively hides the **virus** during the **scan** process. Untouchable 1.1 tricks the virus so it cannot detect the scanning process while it is being performed.

-- Archived File Scanning -- Untouchable 1.1...

30/3,K/45 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

07052176 Supplier Number: 58370810 (USE FORMAT 7 FOR FULLTEXT)
Deploying Enterprise-wide Virus Protection. (Industry Trend or Event)
ENT, v11, n2, p2S1
July 16, 1997
Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Professional
Word Count: 5182

... Polymorphic Virus--Changes its signature, or profile, each time it is activated so that a fixed signature filter will miss it as it does its **virus scan** .

* Stealth **Virus** --Attempts to hide its presence by **intercepting** interrupt services and by feeding back false **information** to virus protection products and end users.

* Encrypted Virus--Delivered within an encrypted file, undetectable by a simple **virus** protection **scan** .

Alarming Growth Rate
Although a

30/3,K/46 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

05884660 Supplier Number: 53070606 (USE FORMAT 7 FOR FULLTEXT)
E-mail: Another network headache?
Mendler, Camille
CommunicationsWeek International, p6(1)
Sept 21, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1433

... policy and procedures regarding Internet use, they tend to be weighted toward technical issues: Historically the IS department has taken a lead in this area, **preventing** the download of computer **viruses** and trying to **intercept** large **files** that might overload the e-mail system. The equally likely potential for infringing copyright, circulating offensive material and making defamatory or libelous statements falls further...

30/3,K/47 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

01447885 Supplier Number: 41737444 (USE FORMAT 7 FOR FULLTEXT)
Norton's backup, antivirus products
Computer Reseller News, p10
Dec 17, 1990
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 114

... 2.
The antivirus product is akin to Symantec's virus protection package for Apple Computer Inc.'s Macintosh. It offers a menu-driven interface and **scans** for **viruses** on either a local or network drive. The primary feature, Virus **Intercept**, examines every new **file** introduced to the system.
The new version of Norton Backup is designed to offer faster backup and restore, increased compatibility with non-standard hardware environments...

30/3,K/48 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2004 The Gale Group. All rts. reserv.

01330281 Supplier Number: 41566881
Norton Antivirus Detects, Intercepts DOS PC Viruses
PC Week, p32
Sept 24, 1990
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Tabloid; General Trade

ABSTRACT:
...floppy disk or a network file server. The program, which integrates protection, detection, and eradication into a single package, features a 17-Kbyte memory resident '**virus intercept**' function that **checks** each application and **file** that is loaded into memory. The utility, which was developed by recently acquired Peter Norton Group, is targeted at firms that presently have no protection...

30/3,K/49 (Item 1 from file: 160)
DIALOG(R)File 160:Gale Group PROMT(R)
(c) 1999 The Gale Group. All rts. reserv.

02219381
SAM safeguards Mac against virus invasions
Canadian Datasystems June, 1989 p. 21
ISSN: 0008-3364

Symantec Canada (Waterloo, ON) is providing Symantec AntiVirus for Macintosh (SAM), a software package, that detects and **eliminates** computer **virus** programs and related **file** damage. The product consists of **Intercept**, a run-time concept software safeguard designed to **prevent** take-up of **viral** programming, and **Virus Clinic** that repairs or **deletes** files already damaged by known **viruses**. There are 4 protection layers to guard against amateur and professional saboteurs and includes a

learn mode so that desirable programming that resembles viral activity...

30/3,K/50 (Item 1 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

10575019 SUPPLIER NUMBER: 21204306 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Do your computers catch colds?(computer viruses)
Tyler, Geoff
Management Accounting (British), v76, n9, p42(2)
Oct, 1998
ISSN: 0025-1682 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2165 LINE COUNT: 00229

... improve, so criminal methods improve to overcome them.
Viruses can now change their signatures--polymorphic viruses--each time they are activated so a fixed signature **filter** will miss them. Other, stealth, **viruses intercept** interrupts and feed false **information** to **virus scanners** and their users. Yet others have their own encrypted files which, again, some simple older scanners will miss.
According to Richard Fern, security business manager...

30/3,K/51 (Item 2 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09826672 SUPPLIER NUMBER: 19944026 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Integralis' MIMESweeper Brings Content Security to Lotus Notes Sites
PR Newswire, pl103SFM026
Nov 3, 1997
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 478 LINE COUNT: 00047

... now benefit from centralized management of the e-mail and web traffic within their networks."
MIMESweeper v3.1 runs on Windows NT 4.0. It **prevents viruses** within emails or FTP and HTTP **files** from reaching users by automatically **intercepting** all inbound and outbound messages from and within a Lotus Notes server. MIMESweeper breaks data into its simplest form before analyzing the content, revealing hidden...

30/3,K/52 (Item 3 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

09175043 SUPPLIER NUMBER: 18936175 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Be prepared to thwart viruses. (anti-virus software for networks)
(Technology Information)
Bryne, Jason
Government Computer News, v15, n29, p29(2)
Nov 18, 1996
ISSN: 0738-4300 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1036 LINE COUNT: 00083

... whether by virus scanning or backup, doesn't work if it you do it occasionally. If you can find a server or desktop program that **intercepts viruses** and constantly **scans** any **file** that is accessed, you'll have more protection.
This takes up system resources, but depending on the system and how it's used, it usually...

30/3,K/53 (Item 4 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2004 The Gale Group. All rts. reserv.

08046590 SUPPLIER NUMBER: 17124859 (USE FORMAT 7 OR 9 FOR FULL TEXT)
**SYMANTEC ANTIVIRUS FOR MACINTOSH DETECTS AND PROTECTS AGAINST NEW HC 9507
VIRUS**

PR Newswire, p804LA012

August 4, 1995

LANGUAGE: English RECORD TYPE: Fulltext

WORD COUNT: 490 LINE COUNT: 00052

... 0 and 3.5 customers can immediately update the detection and capabilities of the program against this new virus by downloading the updated virus definition **file** onto their system. Once updated, **SAM Intercept** and **SAM Virus Clinic** will detect and **eliminate** the **virus** from any infected HyperCard stacks. Note: Because the HC 9507 virus overwrites stack resources as part of its infection, a repaired stack may not run...

30/3,K/54 (Item 5 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2004 The Gale Group. All rts. reserv.

06511420 SUPPLIER NUMBER: 14508979 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Virus protection program. (Software Review) (Evaluation)

Primich, Tracy

Library Software Review, v12, n2, p93(3)

Summer, 1993

DOCUMENT TYPE: Evaluation ISSN: 0742-5759 LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT

WORD COUNT: 1205 LINE COUNT: 00090

... the Virus Definitions File. The Virus Definitions File was new to SAM 3.0. This file is essential to both the Virus Clinic and **SAM Intercept**, since both refer to the **Virus Definitions File** when **scanning** for **viruses**. When new **viruses** are detected and deciphered, Symantec updates the Virus Definitions File. So should you. There are several options. You can call Symantec and order a new...

30/3,K/55 (Item 6 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2004 The Gale Group. All rts. reserv.

06132570 SUPPLIER NUMBER: 12677887 (USE FORMAT 7 OR 9 FOR FULL TEXT)

**Intel Corp.'s antivirus tool shields NetWare domains. (LANProtect 1.5
upgrade includes virus-detection software) (Product Announcement)**

Olsen, Florence

Government Computer News, v11, n19, p40(1)

Sept 14, 1992

DOCUMENT TYPE: Product Announcement ISSN: 0738-4300 LANGUAGE:

ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT

WORD COUNT: 368 LINE COUNT: 00029

... NLM and NetWare file types from any MS-DOS, Microsoft Windows, Apple Macintosh or OS/2 network station.

"Any traffic that can go through the **file** server can be **intercepted** by the LANProtect NLM and **scanned** for **viruses**," said Brett Walker, senior product marketing engineer for Intel.

Walker said the new version is better at detecting polymorphic viruses and stealth viruses, which attach...

30/3,K/56 (Item 7 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2004 The Gale Group. All rts. reserv.

06081196 SUPPLIER NUMBER: 12322406 (USE FORMAT 7 OR 9 FOR FULL TEXT)

SYMANTEC ANNOUNCES ANTIVIRUS FOR MACINTOSH TROJAN HORSE

PR Newswire, 0709A7931

July 9, 1992

LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

WORD COUNT: 355 LINE COUNT: 00030

... Horse by entering the new virus definition into SAM Virus Clinic. In conjunction with the new SAM User Definition and SAM 3.0, users can **scan** for ChinaTalk from both **Virus Clinic** and **SAM Intercept**.

To detect and repair infected **files**, users can download the new virus definitions file free of charge from the Symantec Bulletin Board at 408-973-9598, CompuServe, America Online and Applelink...

30/3,K/57 (Item 8 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2004 The Gale Group. All rts. reserv.

05918763 SUPPLIER NUMBER: 12509830 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Coping with computer viruses: general discussion and review of Symantec

Anti - Virus for the Macintosh.

Primich, Tracy

Library Software Review, v11, n2, p9(4)

March-April, 1992

DOCUMENT TYPE: evaluation ISSN: 0742-5759 LANGUAGE: ENGLISH

RECORD TYPE: FULLTEXT

WORD COUNT: 2438 LINE COUNT: 00186

... a folder, disk, or entire hard drive, alerts the user to the presence to viruses and, when directed by the user. repairs or deletes infected **files**. **SAM Intercept** is an INIT that **monitors** the system for suspicious, **virus** -like activity. I tested both SAM Virus Clinic and SAM Intercept, and both accurately and efficiently detected the Scores Intercept, and both accurately and infected...the virus identifiers known to Symantec at the time when the file was created. This file is essential because both SAM Virus Clinic and **SAM Intercept** use the **Virus Definitions File** when **scanning** for **viruses** and repairing infected files. When new **viruses** are **identified** by Symantex, the **Virus Definitions File** must be updated in order for SAM to recognize are busy beavers, new viruses are not an uncommon discovery. In order for SAM...

30/3,K/58 (Item 9 from file: 148)

DIALOG(R)File 148:Gale Group Trade & Industry DB

(c)2004 The Gale Group. All rts. reserv.

05775754 SUPPLIER NUMBER: 11815250 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Protecting the vulnerable CD-Rom workstation: safe computing in an age of computer viruses.

Flanders, Bruce

CD-ROM Librarian, v7, n1, p26(4)

Jan, 1992

ISSN: 0893-9934 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT

WORD COUNT: 2070 LINE COUNT: 00167

... brought onto or taken off the PC to protect against infected files entering the system through a floppy disk or across a network. In addition, **Virus Intercept checks** every application and every **file** that the application attempts to load into memory. Virus Intercept will alert users to virus attacks with Windows or any graphic mode application running.

Virus...

30/3,K/59 (Item 1 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2004 ProQuest Info&Learning. All rts. reserv.

01473273 01-24261

Cleansing your computer's palate

Thompson, Amy

Security Management v41n7 PP: 101-105 Jul 1997

ISSN: 0145-9406 JRNL CODE: SEM

WORD COUNT: 2080

...TEXT: SMTP) server as well as information transfer through HTTP and FTP servers.

InterScan VirusWall checks all incoming file extensions and headers. When it detects a **file** capable of containing a virus, VirusWall **intercepts** the contents of the **file** and stores it on a temporary file on the gateway machine. It then invokes the **virus - checking** program.

E-mail attachments are opened and scanned before they enter the internal network, where they are encrypted by the various mail systems such as...

30/3,K/60 (Item 2 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2004 ProQuest Info&Learning. All rts. reserv.

00819098 94-68490

SAM 3.5.8

Steinberg, Gene

Macworld v11n3 PP: 68 Mar 1994

ISSN: 0741-8647 JRNL CODE: MAW

WORD COUNT: 660

...TEXT: includes SAM Intercept Jr., which offers basic virus protection but none of the extensive configuration options offered by its bigger sibling.

SAM Virus Clinic extends **virus** protection by offering scheduled **scans**. It can also inoculate your software, which provides SAM **Intercept** with **information** it needs to determine whether an application has changed since it was last launched. During my tests, I found that applications as diverse as America...

30/3,K/61 (Item 3 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

(c) 2004 ProQuest Info&Learning. All rts. reserv.

00728024 93-77245

VARs Find Profit in Crime

Trowbridge, Dave

Computer Technology Review v12n8 PP: 1, 8, 11 Jul 1992

ISSN: 0278-9647 JRNL CODE: CTN

WORD COUNT: 1846

...TEXT: size. Signature detection depends on identifying a piece of viral code in the infected file, and requires frequent updates from the supplier of the anti-**virus** program.

Activity **monitoring** looks for suspicious behavior (trying to write to the COMMAND.COM **file**, attempts to format the disk, etc.) and **intercepts** them. ...

30/3,K/62 (Item 1 from file: 647)

DIALOG(R)File 647:CMP Computer Fulltext

(c) 2004 CMP Media, LLC. All rts. reserv.

01117571 CMP ACCESSION NUMBER: WIN19970201S0106

Head To Head: Antivirus Software - Practice Safe Software

Lenny Bailes

WINDOWS MAGAZINE, 1997, n 802, PG126

PUBLICATION DATE: 970201

JOURNAL CODE: WIN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: WinLab Reviews - What's Hot!
WORD COUNT: 1524

... virus-like code and activity. The efficiency of these tools varied from one product to the next. IBM's AntiVirus 2.5, for example, inconsistently **intercepted** copy operations with infected **files**. Not until options in the Scanner's Setup menu had been turned on did it detect the Concept **virus**. It successfully **prevented** attaching or decoding infected Word documents in e-mail messages; however, it didn't guard against attaching or decoding files infected with the DOS Ambulance virus. Although the **intercept** screen warned that the **file** was infected, it allowed the plagued program to continue.

The Parsons ViruCide Plus Active **Monitor** performed better but displayed constant **virus** -interception messages rather than just beeping once and allowing me to cancel the operation. With the exception of the Lupin and Moonlite.458 **viruses**, Active **Monitor** successfully **intercepted** attempts to attach infected **files** to e-mail messages or unpack already received infected attachments.

No virus was safe from Dr Solomon's WinGuard, which intercepted every one tested. The...

30/3,K/63 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2004 CMP Media, LLC. All rts. reserv.

00577972 CMP ACCESSION NUMBER: CRN19901217S0506

Norton's backup, antivirus products
COMPUTER RESELLER NEWS, 1990, n 399, 10
PUBLICATION DATE: 901217
JOURNAL CODE: CRN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: NEWS
WORD COUNT: 114

... 2.
The antivirus product is akin to Symantec's virus protection package for Apple Computer Inc.'s Macintosh. It offers a menu-driven interface and **scans** for **viruses** on either a local or network drive. The primary feature, Virus **Intercept**, examines every new **file** introduced to the system.

File 8: Ei Compendex(R) 1970-2004/Jul W3
(c) 2004 Elsevier Eng. Info. Inc.
File 35: Dissertation Abs Online 1861-2004/May
(c) 2004 ProQuest Info&Learning
File 202: Info. Sci. & Tech. Abs. 1966-2004/Jul 12
(c) 2004 EBSCO Publishing
File 65: Inside Conferences 1993-2004/Jul W3
(c) 2004 BLDSC all rts. reserv.
File 2: INSPEC 1969-2004/Jul W3
(c) 2004 Institution of Electrical Engineers
File 233: Internet & Personal Comp. Abs. 1981-2003/Sep
(c) 2003 EBSCO Pub.
File 94: JICST-EPlus 1985-2004/Jul W1
(c) 2004 Japan Science and Tech Corp(JST)
File 483: Newspaper Abs Daily 1986-2004/Jul 23
(c) 2004 ProQuest Info&Learning
File 6: NTIS 1964-2004/Jul W4
(c) 2004 NTIS, Intl Cpyrght All Rights Res
File 144: Pascal 1973-2004/Jul W3
(c) 2004 INIST/CNRS
File 434: SciSearch(R) Cited Ref Sci 1974-1989/Dec
(c) 1998 Inst for Sci Info
File 34: SciSearch(R) Cited Ref Sci 1990-2004/Jul W3
(c) 2004 Inst for Sci Info
File 99: Wilson Appl. Sci & Tech Abs 1983-2004/Jun
(c) 2004 The HW Wilson Co.
File 583: Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
File 266: FEDRIP 2004/Jun
Comp & dist by NTIS, Intl Copyright All Rights Res
File 95: TEME-Technology & Management 1989-2004/Jun W1
(c) 2004 FIZ TECHNIK
File 438: Library Lit. & Info. Science 1984-2004/Jun
(c) 2004 The HW Wilson Co
File 256: SoftBase: Reviews, Companies & Prods. 82-2004/Jun
(c) 2004 Info.Sources Inc

Set	Items	Description
S1	1051146	VIRUS?? OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE?? OR WORM?? OR (MALICIOUS OR HOSTILE OR SUSPECT) () (LOGIC OR CODE OR SOFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ? OR DATA OR INFORMATION OR PACKET? ?)
S2	100630	ANTIVIRUS OR ANTIVIRAL
S3	57515	S1(5N) (SCAN???? OR MONITOR??? OR CHECK??? OR INTERCEPT? OR PREVENT? OR IDENTIF? OR RECOGNI????? OR REMOV??? OR DELET??? OR ELIMINAT? OR ERAS??? OR ERADICAT??? OR FILTER???)
S4	2802	INTERCEPT???(7N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ? OR CONTENT OR DATA OR INFORMATION)
S5	137725	PORTAL? ? OR GATEWAY? ?
S6	3	S3 AND S4 AND S5
S7	1	S2 AND S4 AND S5
S8	6	S1 AND S4 AND S5
S9	73	S1:S2 AND S4
S10	48	S2:S3 AND S4
S11	50	S6:S8 OR S10
S12	48	RD (unique items)
S13	22	S12 NOT PY=2001:2004
S14	8	ESAFE()GATEWAY
S15	6	RD (unique items)
S16	6	S15 NOT S13
S17	2	S16 AND PY=2000

13/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:EI Compendex(R)
(c) 2004 Elsevier Eng. Info. Inc. All rts. reserv.

04935096 E.I. No: EIP98024056537

Title: Getting started on the net

Author: Herbert, Simon

Source: Computer Bulletin (London, 1986) v 9 n pt 6 Dec 1997. p 28-29

Publication Year: 1997

CODEN: CBULEW ISSN: 0010-4531

Language: English

Document Type: JA; (Journal Article) Treatment: G; (General Review)

Journal Announcement: 9804W2

Abstract: There are four areas to be investigated before starting to build an Internet access. These include: connection to the Internet; e-mail; a World Wide Web site; and security. To connect to the Internet, an Internet service provider (ISP) that will offer a telephone number, a user ID and a password is needed. After having an ISP, a modem is needed to have access to Internet services. Having access, the e-mail is the most useful aspect of the Internet. In an e-mail service, all users should have their own personal ID. Setting up a Web site can be divided into five main steps: investigation; domain registration; page design; construction; and updating search engines. The security issues are: unauthorized access; **information interception**; and **viruses**.

Descriptors: *Wide area networks; Information services; Modems; Electronic mail; Security of data; Personal computers; Data communication systems; Computer viruses; Network protocols

Identifiers: Internet service providers (ISP); World wide web (WWW); Post office protocols (POP); Simple mail transfer protocols (SMTP)

Classification Codes:

722.3 (Data Communication, Equipment & Techniques); 903.4 (Information Services); 723.5 (Computer Applications); 723.2 (Data Processing); 722.4 (Digital Computers & Systems)

722 (Computer Hardware); 903 (Information Science); 723 (Computer Software)

72 (COMPUTERS & DATA PROCESSING); 90 (GENERAL ENGINEERING)

13/5/2 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

4796476

Title: Sophos Intercheck (anti-virus software)

Journal: LAN Magazine vol.2, no.10 p.20, 22

Publication Date: Oct. 1994 Country of Publication: UK

CODEN: LMAGEP ISSN: 0968-6320

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P); Product Review (R)

Abstract: The Sophos Intercheck TSR complements the Sweep anti-virus NLM and is the first such package capable of **checking** for polymorphic **viruses**. Although it can be used on standalone PCs, this TSR is really aimed at network workstations. The Intercheck TSR is usually loaded across the network from the file server by the system login script. Nevertheless, it is a TSR. Its function is to **intercept** any call to copy or execute a **file** and **check** it for possible **virus** infection. The TSR occupies 23Kb of memory. (0 Refs)

Subfile: D

Descriptors: computer viruses; program debugging; software packages

Identifiers: Sophos Intercheck; TSR; Sweep anti-virus NLM; polymorphic viruses; network workstations; file server; system login script; virus infection; terminate-and-stay-resident

Class Codes: D1060 (Security); D2000 (Applications)

13/5/3 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC
(c) 2004 Institution of Electrical Engineers. All rts. reserv.

03923947 INSPEC Abstract Number: C91048431

Title: Virus -specific monitoring programs

Journal: Virus Bulletin p.6-7

Publication Date: May 1991 Country of Publication: UK

CODEN: VBULE3 ISSN: 0956-9979

U.S. Copyright Clearance Center Code: 0956-9979/90/\$0.00+2.50

Language: English Document Type: Journal Paper (JP)

Treatment: Practical (P)

Abstract: Just like **virus scanners**, all **virus -specific monitoring** programs are only effective against known viruses. Consequently, frequent updates are necessary to keep them current as new **viruses** appear. Several different types of **monitoring** program exist, but they all have certain features in common, such as a database of **information** about the **viruses** they are intended to **intercept**. Unfortunately this database grows as the number of viruses increases, usually with a corresponding increase in the memory requirements of these programs. There are a number of different **virus -specific monitors** which adopt various modi operandi. Some **virus -specific monitors** incorporate all of the scanning routines while others use only one **interception** method. The **article** discusses disk scanning, scanning on program execution, interrupt functions and provides a list of IBM PC viruses. (0 Refs)

Subfile: C

Descriptors: computer viruses; supervisory programs

Identifiers: **virus -specific monitoring** programs; database; scanning routines; interception method; disk scanning; interrupt functions; IBM PC viruses

Class Codes: C6150J (Operating systems); C6130 (Data handling techniques)

13/5/4 (Item 3 from file: 2)

DIALOG(R)File 2:INSPEC

(c) 2004 Institution of Electrical Engineers. All rts. reserv.

03527538 INSPEC Abstract Number: C90004789

Title: Response to the Law Commission's Working Paper no.110, computer misuse

Journal: Computer Law & Practice vol.5, no.5 p.185-9

Publication Date: 1989 Country of Publication: UK

CODEN: CLPRER ISSN: 0266-4801

Language: English Document Type: Journal Paper (JP)

Treatment: General, Review (G)

Abstract: The article presents the response of the Society for Computers and Law to the Law Commission's Working Paper no.110 concerning computer misuse. The scope of the general criminal law for dealing with computer misuse is discussed. Computer fraud, computer hacking, unauthorised access and use, dishonest programming (**viruses**), unauthorised **deletion** of computer **information**, unauthorised **interception** of computer signals etc. are also covered. (0 Refs)

Subfile: C

Descriptors: computer crime; government policies; legislation; security of data

Identifiers: Law Commission Working Paper no.110; computer fraud; unauthorised use; computer viruses; unauthorised signal interception; unauthorised data deletion; Society for Computers and Law; computer misuse; general criminal law; computer hacking; unauthorised access; dishonest programming

Class Codes: C0230B (Legal aspects)

13/5/5 (Item 1 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00616678 00NC12-007

Aladdin puts content-borne viruses back in the bottle

DeMaria, Michael J

Network Computing , December 4, 2000 , v11 n24 p32-34, 2 Page(s)

ISSN: 1046-4468

Company Name: Aladdin Knowledge Systems

URL: <http://www.eAladdin.com>

Product Name: eSafe **Gateway**

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): B

Geographic Location: United States

Presents a favorable review of eSafe **Gateway** (\$1,500), content security software from Aladdin Knowledge Systems (800, 847). Explains that it scans files and Web pages for malicious content, providing an effective way to stop macro **viruses** , **Trojan horses** , and malicious Java applets in their tracks. Highlights its **Content Redirector gateway** device that **intercepts** traffic and routes it to a **Content Inspector** machine, eConsole management graphical user interface, integration with existing network protection devices, load-sharing and failover capabilities, and protection for File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Simple Mail Transfer Protocol (SMTP) traffic. Mentions, however, that bugs were encountered during testing. Concludes that it is a useful addition to an established protection system. Includes a screen display and a product summary. (MEM)

Descriptors: **Gateway** ; Security Measures; Network Security;

Antivirus Software; Privacy Protection; File Management; **Virus**

Identifiers: eSafe **Gateway** ; Aladdin Knowledge Systems

13/5/6 (Item 2 from file: 233)

DIALOG(R) File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00552263 99MQ11-007

Protect thy notebook; SOS Best Defense

Compton, Jason

Mobile Computing & Communications , November 1, 1999 , v10 n11 p34, 1

Page(s)

ISSN: 1047-1952

Company Name: Sterling Strategic Solutions

URL: <http://www.sterlingweb.com>

Product Name: SOS Best Defense

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): B

Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows

Geographic Location: United States

Presents a favorable review of SOS Best Defense (\$60), a notebook computer protection system from Sterling Strategic Solutions of Houston, TX (800). Runs on Windows. Explains that it combines system administration, an Internet filter, and **antivirus** utility. Cites features such as configurability for an unlimited number of users, ability to shut down Java or ActiveX applets before they launch, blocking of key words in downloading, designation of approved Web sites, mouse-click disabling of individual devices and Windows functions, and **interception** of potentially hazardous **files** . Reports, however, that in default mode, the program gave off more than one false alarm. Concludes that ``while dedicated hooligans will find ways to get around the SOS Best Defense system, it deters casual users from doing things they shouldn't.'' Includes one product summary and one screen display. (MEM)

Descriptors: Security; **Filtering** ; **Virus** ; Mobile Computing; Portable Computer; Laptop Computers

Identifiers: SOS Best Defense; Sterling Strategic Solutions

13/5/7 (Item 3 from file: 233)

DIALOG(R) File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00516761 98IX12-001

The year in review -- With '99 right around the corner, it's wise to heed the old adage, ``Those who cannot remember the past are condemned to repeat it''

Kabay, M E

Information Security , December 1, 1998 , v1 n13 p16-22, 7 Page(s)

ISSN: 1096-8903

Languages: English

Document Type: Articles, News & Columns

Geographic Location: United States

Asserts that confidentiality, control (or possession), integrity, authenticity, availability, and utility are the six fundamentals of information security. Discusses some causes of information security glitches and violations, such as **data** diddling, data corruption, wiretapping and **interception** , **viruses** , hoaxes and trojans, and fraud, extortion, and slamming. Recounts incidents where each occurred and the circumstances surrounding each occurrence. Talks about such information security concerns as theft of equipment, theft of identity, denial of service, and Web attacks. Notes that methods are being developed that are intended to defeat encryption. Concludes that carelessness, lack of normal controls like separation of duties, and missed security software updates are often the cause of any security-related problems. Includes one illustration. (CAT)

Descriptors: Information Management; Information Policy; Law Enforcement; Virus; Encryption; Security

13/5/8 (Item 4 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00504856 98SR08-007

Electronic access security -- Beam me up, Scottie

SC/INFO SECURITY NEWS MAGAZINE , August 1, 1998 , v9 n8 p38-44, 7 Page(s)

ISSN: 1096-7974

Company Name: Content Technologies; AbirNet; TenFour

URL: <http://www.mimesweeper.com> <http://www.abirnet.com> <http://www.tenfour.com>

Product Name: MIMESweeper 3.2 1; SessionWall-3 2.1; TFS **Gateway** 3.1

Languages: English

Document Type: Buyer and Vendor Guide

Geographic Location: United States

Presents a buyers' guide to nine electronic access security products from nine manufacturers, citing three of these as SC Magazine Best Buys due to their success in attempting to both ban access to a network, as well as monitor network situations and report on them. Notes that MIMESweeper v3.2 1 (\$NA) from Content Technologies (425) tackles both e-mail and Web problems, **intercepting viruses** and **checking** for unacceptable content , which can then be filtered out of the incoming data stream. Indicates that SessionWall-3 v2.1 (\$1,495) from AbirNet (817) is a heavyweight program which is nonetheless easy to install and use, calling it a great product for monitoring and defending a network and its users against both internal and external abuses. States that TFS **Gateway** v3.1 (\$NA) from TenFour (800) is well designed, and adds spam **filtering** , **virus scanning** , encryption, and mail message tracking to an e-mail system. Includes 10 photos, two screen displays, one sidebar, and nine ratings tables.

Descriptors: Security; Internet; Network Management; Networks; **Virus** ; Electronic Mail; **Filtering**

Identifiers: MIMESweeper 3.2-1; SessionWall-3 2.1; TFS **Gateway** 3.1; Content Technologies; AbirNet; TenFour

13/5/9 (Item 5 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00450004 97WN02-004

Practice safe software -- HEAD TO HEAD: antivirus software

Bailes, Lenny

Windows Magazine , February 1, 1997 , v8 n2 p126-132, 2 Page(s)

ISSN: 060-1066

Company Name: Symantec; Dr Solomon's Software; Parsons Technology; IBM Corp.

Product Name: Norton **AntiVirus** 2.0; Dr Solomon's Anti-Virus Toolkit 7.64; Parsons ViruCide Plus 4.2; IBM **AntiVirus** 2.5

Languages: English

Document Type: Buyer and Vendor Guide

Grade (of Product Reviewed): A; B; B; C

Hardware/Software Compatibility: IBM PC Compatible; Microsoft Windows; Microsoft Windows 95; Microsoft Windows NT

Geographic Location: United States

Presents a buyers' guide to four **antivirus** programs for IBM PC compatibles with Windows 3.x, 95, or NT. Favorably reviews Dr Solomon's Anti-Virus Toolkit, 7.64 (\$85) from Dr Solomon's Software (617), and Parsons ViruCide Plus 4.2 (\$29) from Parsons Technology; very favorably reviews Norton **AntiVirus** 2.0 (\$69) from Symantec (800, 408); and presents a mixed review of IBM **AntiVirus** 2.5 (\$49) from IBM Corp. (800, 512). Notes that each includes a watchdog utility that seeks virus-like code and activity. Says IBM's **AntiVirus** inconsistently **intercepted** copy operations with infected files, while Dr Solomon's **intercepted** every **virus** tested. Adds that Norton has an easy-to-use disk-monitoring utility. Rates Dr Solomon's three and one-half windows out of five, ViruCide three windows, IBM **AntiVirus** two and one-half windows, and Norton **AntiVirus** four windows and the WINDOWS Magazine Recommended seal. Includes four screen displays and four product summaries. (jo)

Descriptors: Virus; Software Review; Window Software; Security; Disk Files; Utility Program

Identifiers: Norton **AntiVirus** 2.0; Dr Solomon's Anti-Virus Toolkit 7.64; Parsons ViruCide Plus 4.2; IBM **AntiVirus** 2.5; Symantec; Dr Solomon's Software; Parsons Technology; IBM Corp.

13/5/10 (Item 6 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00315807 93MW06-024

Safe & Sound

Angus, Jeffrey Gordon

Macworld , June 1, 1993 , v10 n6 p156, 1 Page(s)

ISSN: 0741-8647

Company Name: Central Point Software

Product Name: Safe & Sound

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): c

Hardware/Software Compatibility: Macintosh Plus

Geographic Location: United States

Presents a mixed review of Safe & Sound (\$49.95), a utility program from Central Point Software (503). The program requires a Macintosh Plus with 2MB RAM and System 6.0.5. The floppy disk can provide recovery for users who are not getting a "'clean boot,'" evidenced by a blinking question mark on the disk icon, the "'sad Mac'" icon, or the Finder not recognizing the drive. It also checks boot blocks and the volume information block, analyzes the catalog tree and the extents tree, and check for bad blocks. It does not back up or defrag **files** and does not provide **virus interception** , but since these features are not required by all users, eliminating them from the package keeps the price low. The program has a clean interface. A good choice for novice users, the package is not complete enough for power users or those who want an all-in-one package. (djd)

Descriptors: Utility Program; Software Review

Identifiers: Safe & Sound; Central Point Software

13/5/11 (Item 7 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00250890 91PI10-144

The Norton AntiVirus

Pastrick, Greg

PC Magazine , October 29, 1991 , v10 n18 p233, 237, 2 Page(s)

ISSN: 0888-8507

Company Name: Symantec

Product Name: Norton **AntiVirus** , The

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): b

Geographic Location: United States

Presents a favorable review of The Norton **AntiVirus** (\$129.95), an **antivirus** utility from Symantec Corp., Cupertino, CA (800, 408). The program requires 384K RAM and DOS 2.0 or later. The package includes a TSR, **Virus Intercept** , that creates 'inoculated files ,' hidden system files protected against viral attack. Depending on the level of protection selected, these files require from 1K to 32K of RAM for monitoring. The program uses checksums to check the integrity of protected files, and this requires a 77-byte check file on disk for each protected file. In testing, the program performed well, although it could not detect or **remove** the Red Cross **virus** or the Totally Hidden **virus** , although it **prevented** the latter from being introduced to the system. The program is easy to use and full-featured, but it cannot scan compressed files and its memory requirements for hidden files is a drawback. Includes one screen display. (djd)

Descriptors: Virus; Security; Software Review

Identifiers: Norton **AntiVirus** , The; Symantec

13/5/12 (Item 8 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00250886 91PI10-140

Data Physician Plus

Fersko-Weiss, Henry

PC Magazine , October 29, 1991 , v10 n18 p217, 1 Page(s)

ISSN: 0888-8507

Company Name: Digital Dispatch

Product Name: Data Physician Plus

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): b

Geographic Location: United States

Presents a favorable review of Data Physician Plus 1.3C (\$49), an **antivirus** utility program from Digital Dispatch Inc., Lakeland, MN (800, 612). The program requires 20K to 256K RAM and DOS 2.0 or later. It is a collection of eight different programs. The main three are Resscan, which monitors files, the boot sector, and memory for viruses; VirAlert, which resides in CONFIG.SYS and **intercepts** attempts to manipulate executable and operating-system files ; and VirHunt, a **scanner** that **removes** most known **viruses** . In testing, the program **prevented** infection by all the test **viruses** except Joshi, and was able to block the Totally Hidden **Virus** . It was able to **remove** all the text **viruses** except Red Cross, which was unknown to the vendor's programmers. Only problem with the package is that the variety of programs is not well documented, and the user will have to do a little work to figure out how to use them. (djd)

Descriptors: Virus; Security; Software Review

Identifiers: Data Physician Plus; Digital Dispatch

13/5/13 (Item 9 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.
(c) 2003 EBSCO Pub. All rts. reserv.

00248503 91LK09-008

VirusCure intercepts **sabotaged** files

Sherman, Tom

LINK-UP , September 1, 1991 , v8 n5 p5, 8, 2 Pages

ISSN: 0073-9988

Company Name: International Microcomputer Software

Product Name: VirusCure Plus

Languages: English

Document Type: Software Review

Grade (of Product Reviewed): B

Hardware/Software Compatibility: IBM PC; IBM PC Compatible

Geographic Location: United States

Presents a favorable view of VirusCure Plus (\$99.95), an anti-virus program from International Microcomputer Software (IMSI), San Rafael, CA (415). Runs on any MS-DOS machine and occupies 25K of memory. Program is designed to **recognize** and cure more than 540 **virus** strains and to guard against future virus infection. Says that installation is easy. Notes that upgrades will be needed to **recognize** new **viruses** . Questions about the program sent to IMSI's bulletin board went unanswered for three weeks, but a toll call to IMSI received clear answers. (SM)

Descriptors: Virus; Security; Software Review

Identifiers: VirusCure Plus; International Microcomputer Software

13/5/14 (Item 10 from file: 233)

DIALOG(R)File 233:Internet & Personal Comp. Abs.

(c) 2003 EBSCO Pub. All rts. reserv.

00176746 88CP09-018

Vaccine

Parker, Tim

Computer Language , September 1, 1988 , v5 n9 p131-132

Languages: English

Document Type: Software Review

Geographic Location: United States

Presents a favorable review of Vaccine (\$189), a virus protection system from FoundationWare, Cleveland, OH (216). The program runs as a TSR requiring 1K RAM and **intercepts** all **file** modifications not approved during installation. It also creates a copy of the disk FAT and partition tables, checks the hard disk for suspect files, virus ``signatures,' and suspicious hidden files. A program for 286- and 386-based computers permits disabling the hard disk while floppy disks are being **checked** for Trojans or **viruses** , an another routine produces a copy of all system information on floppy disk, facilitating recovery of the system in the event an undetected virus destroys it. (djd)

Descriptors: Security; Bugs; Debugging; Software Review

Identifiers: Vaccine; FoundationWare

13/5/15 (Item 1 from file: 99)

DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

(c) 2004 The HW Wilson Co. All rts. reserv.

1140282 H.W. WILSON RECORD NUMBER: BAST94008830

Safeguards on the information highway

Baker, Andrea;

Design News v. 49[50] (Jan. 17 '94) p. 19-20

DOCUMENT TYPE: Feature Article ISSN: 0011-9407 LANGUAGE: English

RECORD STATUS: New record

ABSTRACT: Although they make concurrent engineering possible, networks are increasingly vulnerable to **data** loss through computer **viruses** and electronic **interception** . In response, many computer vendors have created products that improve security, in some cases adapting government products. New security tools that incorporate cryptographic or computer user identification features are described.

DESCRIPTORS: Internetworking; Cryptography; Computer user identification;

13/5/16 (Item 1 from file: 95)

DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01449059 20000904280

Tricksen Sie die Hacker aus. Sicher surfen

Kleinert, J; Schmidt, M; Schroeder, M; Thorbruegge, M
Chip. Computer & Communication, v56, n10,
pp170-174,176,178,180,182-188,190,192-194,196, 2000
Document type: journal article Language: German
Record type: Abstract
ISSN: 0170-6632

ABSTRACT:

Am Thema Datenschutz kommt kein Internet-Surfer vorbei. Der Beitrag versucht, eine systematische Betrachtung der vielfaeltigen Bedrohungen fuer den PC, die von vielen Seiten kommen koennen. Die weit verbreiteten Microsoft-Produkte haben viele Schwachstellen, ueber die E-Mail-Attacken erfolgen koennen. Es werden eine Reihe von Tips und Tricks genannt, wie solche Gefahren abgewehrt werden koennen. In einer Tabelle werden die wichtigsten Antiviren-Programme zusammengestellt. Ein Nutzer sollte sich darueber im klaren sein, dass das Mitlesen von E-Mails nicht schwierig ist. Man sollte daher E-Mails verschluesseln. PGP (pretty good privacy) ist ein Quasistandard fuer sicheres Verschluesseln von E-Mails und anderen Dokumenten im Internet. Dafuer werden praktische Hinweise gegeben. Eine weitere wichtige Frage ist die nach der Sicherheit des Bezahls im Internet und den Risiken bei der Uebermittlung von Kreditkarten-Daten. Schliesslich werden in einem Vergleichstest Firewalls fuer den PC getestet. Dazu sind die Systeme Norton Personal Firewall 2000 von Symantec, eSafe Protect 2.2 (Aladdin), Secure4U (Sandbox Security), McAfee Firewall (McAfee), Surfin Guard 5.0 (Finjan) und Secure Desktop 2.1 (Sybergen) untersucht worden. Testsieger wurde Norton Personal Firewall; das beste Preis-Leistungs-Verhaeltnis wurde eSafe Protect 2.2 zuerkannt.

DESCRIPTORS: DATA INTEGRITY; INTERCEPTION PROTECTION; COMPUTER VIRUSES
; CIPHERING--ENCRYPTION; SAFETY PROGRAM; FIREWALLS; MARKET REVIEW;
PERFORMANCE EVALUATION; VIRUS ANNIHILATION PROGRAM
IDENTIFIERS: Internet-Datenschutz; Sicherheitsmassnahmen; Firewall-Test

13/5/17 (Item 2 from file: 95)

DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01437327 20000802153

Ein Virenschutz macht noch keine Web-Sicherheit. Hacker-Abwehr

anonym
Computer Zeitung, v121, n28, pp19, 2000
Document type: Short journal article Language: German
Record type: Abstract
ISSN: 0341-5406

ABSTRACT:

Derzeit wird beim Thema Web-Security vor allem Denial-of-Service-Attacken und Viren diskutiert. Die Internet-Sicherheit ist jedoch viel komplexer. Nach Erkenntnissen des Darmstaedter Cast-Forums hoert die US-Sicherheitsbehoerde NSA den gesamten Internet-Verkehr ueber Satellit und Seekabel ab. Wirtschaftsspionage spielt offenbar eine grosse Rolle. Ueber trojanische Pferde oder Puffer-Ueberlaeufer, ueber Mail-Anhang oder interaktive Web-Anfrage koennen Server und Anwender-PCs in komplexen Unternehmensnetzen Ziele von Angriffen aus dem Internet sein. Der Beitrag gibt einige Hinweise, wie neben der Absicherung des Web-Verkehrs auch der Schutz von Servern und PCs zum Bestandteil eines umfassenden Sicherheitskonzepts gemacht werden sollte. Bei Clients sollten alle vorhandene Sicherheitsfunktionen aktiviert werden (Passwortschutz,

Makrovirenwarnung in Word und Excel). Die Sicherheit im Browser ist auf die hoechste Stufe einzustellen (Deaktivierung aktiver Inhalte wie Active X und Javascript). Das automatische Starten von Mail-Anhaengen ist zu unterbinden. Bei Servern sollte eine zentrale Ueberpruefung der E-Mails durch Antivirensoftware am Mail-Server/ **Gateway** erfolgen. Filterregeln am Firewall/Mail-Gatewaykoennen gefaehrliche Anhaenge automatisch blocken. Der Server ist mit Blick auf Sicherheitsaspekte zu konfigurieren.

DESCRIPTORS: **DATA INTEGRITY**; **INTERCEPTION PROTECTION**; ACCESS CONTROL; COMPUTER CRIME; COMPUTER **VIRUSES** ; SAFETY SYSTEMS; CLIENT SERVER SYSTEMS; BROWSERS; **VIRUS ANNIHILATION PROGRAM**
IDENTIFIERS: Internet-Verkehr; Datensicherheit; Hacker-Abwehr

13/5/18 (Item 3 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01437324 20000802185
Industrielle Kommunikation - aber sicher
Baumann, G; Sporbert, M
Siemens, Nuernberg, D
etz Elektrotechnik und Automation, v121, n13/14, pp8-9, 2000
Document type: journal article Language: German
Record type: Abstract
ISSN: 0948-7387

ABSTRACT:

Beim offenen Internetworking in der industriellen Kommunikation sind vernetzte Computersysteme und datentechnische Einrichtungen ein potentielles Sicherheitsrisiko. Die weltweite Verteilung der Internet-Infrastruktur und Zugriffsmoeglichkeiten durch aussen Stehende erhoehen die Anforderungen zur Sicherstellung von Vertraulichkeit und Integritaet der Daten. Im ersten Teil eines auf drei Teile angelegten Beitrags werden die fuer das Gefahrenpotential aus dem Internet wesentlichen Angriffsarten beschrieben. Zunaechst werden Boot-Viren, File-Viren und trojanische Pferde charakterisiert. Bei Sniffer-Angriffen werden geheime Daten durch Ueberwachung der Datenpakete auf IP-Protokollebene ermittelt. Durch diverse Programme zur Protokollanalyse koennen Angreifer in kuerzester Zeit in Besitz einer grossen Anzahl von Passwoertern oder anderen vertraulichen Informationen kommen. Spoofing ist eine haeufig benutzte Technik zur Ueberwindung von Firewall-Systemen und stellt gleichzeitig die Grundlage fuer eine Reihe weiterer Angriffsmethoden dar. Bei Spoofing verfaelscht der Angreifer die Absender-Adresse der IP-Pakete, um sich als berechtigter Benutzer auszugeben. Gefaehrlich ist diese Form des Angriffs vor allem, wenn als Firewall-System Paketfilter zum Einsatz kommen, die lediglich in der Lage sind, die Herkunft von Datenpaketen anhand der Source-Adresse zu bestimmen. Die Datenpakete werden dabei vermeintlich als von berechtigten Nutzern stammende Pakete behandelt und weitervermittelt. Bei Routing-Angriffen sendet ein Angreifer falsche RIP-Pakete (RIP, Routing Information Protocol). Er kann dadurch gezielt Uebertragungswege manipulieren, unerwuenschte Routen konfigurieren und sicherstellen, dass die Datenpakete zum Mithoeren mit einem Sniffer ueber seinen Rechner laufen. Eine der groessten Gefahren im Internet stellen sogenannte 'Denial of Service-Attacks' dar: Bei diesen Angriffen werden Rechner oder einzelne Dienste im Internet zum Absturz gebracht bzw. Ressourcen ueberbeansprucht, die dann voruebergehend anderen Nutzern nicht zur Verfuegung stehen. Ermoeeglicht werden solche Angriffe unter anderem durch Softwarefehler. Hopping stellt das unerlaubte Weiterspringen von einem Remote-Rechnersystem auf ein weiteres Rechnersystem dar. Dabei werden die Moeglichkeiten des entfernten Systems fuer den Zugriff auf das weitere Rechnersystem genutzt. (Wird fortgesetzt)

DESCRIPTORS: **INTERCEPTION** ; **INTERCEPTION PROTECTION** ; COMPUTER CRIME; COMPUTER **VIRUSES** ; **DATA MISUSE**; **DATA NETWORKS**; DATA INTEGRITY; BACK UP ; FIREWALLS; INFORMATION ACCESS; COMMUNICATION PROTOCOLS; ENTERPRISE--FIRM; WORLD WIDE WEB; BROWSERS
IDENTIFIERS: Internet-Kommunikation; Angriffsarten; Sicherheitsrisiko

13/5/19 (Item 4 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01434652 20000705432

Stand der Technik. Wie funktionieren eigentlich IT-Security-Systeme?

Lamm, A
Strategic Dev., Articon-Integralis, Heilbronn, D
Markt und Technik, v12, n26, pp24,26, 2000
Document type: journal article Language: German
Record type: Abstract
ISSN: 0344-8843

ABSTRACT:

Rund 72 Millionen Rechner sind am Internet angeschlossen und die Tendenz ist steigend. Die Chancen, einen beliebigen Datenverkehr abzuhoeren oder sich ueber das Internet in die internen Netzwerke von Unternehmen einzuschleichen, sind gross. Hinzu kommt, dass die sogenannten Mission-critical-Systeme und die Internet-Zugaenge immer mehr zu einer Einheit verschmelzen. Integritaet, Vertraulichkeit und Verfuegbarkeit der Daten lauten die Anforderungen an eine sichere Umgebung fuer B2B-Kommunikation via Internet. Technisch muessen dabei alle Schichten des TCP/IP-Protokolls abgesichert werden, also von der Netzwerkebene bis hin zur Applikation. Sogenannte Firewalls stellen die Grundversorgung dar, um Eindringlinge vom internen Netzwerk abzuhalten. Ueber Regeln laesst sich einstellen, welcher Internet-Dienst erlaubt ist und welcher nicht. Von Hackern koennen Firewalls ueberwunden werden, in dem sie sich ueber den Dienst E-Mail oder World Wide Web Zugang verschaffen. Zusaetzliche Sicherheit verschaffen Mechanismen wie Authentisierung und digitale Zertifikate. Sie sind zwingend, wenn Geschaeftpartner oder Niederlassungen auf interne Daten zugreifen wollen. Public-Key-Verfahren oder Challenge-Response-Verfahren kommen hierbei zum Einsatz. Beim Transport der Daten ueber das unsichere Internet kommt der Verschluesselung eine wichtige Bedeutung zu. Zum Einsatz kommt hier das Tunneling-Verfahren: In ein IP-Paket wird ein zweites, verschluesseltes Paket gepackt. Der neue IPSEC-Standard gestattet den Aufbau heterogener Verbindungen und loest die Tunnelprotokolle ab. IPSEC sichert dabei zwar die **Gateways** ab, bringt aber auch keine totale Sicherheit. Content-Security und Virenschutz sollten auf keinem System fehlen.

DESCRIPTORS: **INTERCEPTION PROTECTION; COMPUTER VIRUSES ; DATA MISUSE; DATA INTEGRITY; FIREWALLS; INFORMATION TECHNOLOGY; INFORMATION ACCESS; MICROCOMPUTERS; COMPUTER NETWORKS; SMART CARDS; ENTERPRISE--FIRM; CIPHERING --ENCRYPTION; WORLD WIDE WEB; CERTIFICATES; ACCESS PROTOCOLS; INTERNET UNIFIED COMMUNICATIONS PROTOCOL**
IDENTIFIERS: Datenverkehr; uthentisierung

13/5/20 (Item 5 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management
(c) 2004 FIZ TECHNIK. All rts. reserv.

01411681 20000504220

Fenster abdichten. Sicherheits-Tools

Nefzger, W
PC Magazin, Poing, v45, n6, pp88-89, 2000
Document type: journal article Language: German
Record type: Abstract
ISSN: 0933-1557

ABSTRACT:

Im Beitrag werden Sicherheits-Tools vorgestellt, die gegen Manipulationen, Virenattacken und Lauschangriffen aus dem Internet helfen sollen. Es ist aber auch Vorsicht geboten, da durch Sicherheitsvorkehrungen auch Daten vernichtet werden koennen. Deshalb wurden in die Toolsammlung zwei Programme aufgenommen, die als Gegengift zu den vorgestellten

Sicherheits-Utilities wirken. Die Freeware ist unterteilt in Antiviren- und Verschlüsselungs-Tools. Die Programme sind beschrieben und in einer Tabelle mit den Merkmalen Programm, Internet-Adresse, Betriebssystem, Sprache und Gattung gegenuebergestellt.

DESCRIPTORS: WORLD WIDE WEB; SAFETY; **DATA INTEGRITY**; COMPUTER **VIRUSES** ;
COMPUTER CRIME; ACCESS CONTROL; **INTERCEPTION PROTECTION**; PRODUCT
INFORMATION ; SOFTWARE TOOLS
IDENTIFIERS: Internet; Sicherheits-Tool; Freeware; Produktinformation

13/5/21 (Item 1 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2004 Info.Sources Inc. All rts. reserv.

00127248 DOCUMENT TYPE: Review

PRODUCT NAMES: Sophos Anti-Virus for Notes/Domino 2.0 (027952); Antigen for Lotus Notes (775398)

TITLE: Getting Notes Inoculated: Two solutions for keeping viruses out...
AUTHOR: Schultz, Keith
SOURCE: InternetWeek, v840 p62(2) Dec 4, 2000
ISSN: 0746-8121
HOMEPAGE: <http://www.internetwk.com>

RECORD TYPE: Review
REVIEW TYPE: Product Comparison
GRADE: Product Comparison, No Rating

Sophos's Sophos Anti-Virus for Notes/Domino 2.0 and Sybari Software's Antigen for Lotus Notes are reviewed and compared virus 'inoculation' products for user of Lotus Development's Notes. Sophos is easy to install and administer, and offers robust **antivirus** protection. However, Sophos runs only under Notes 4.6.2 on Windows NT/2000 platforms. Antigen's **antivirus** protection is super for all versions of Notes and runs on many operating platforms. However, Antigen's performance degrades when processing messages with multiple attachments. Sophos Anti-Virus for Notes/Domino 2.0 worked without a hitch to detect viruses and provides an uncluttered and logical interface, and CPU utilization with Sophos was less than with Antigen's when processing documents with multiple file attachments. Sophos resides atop a local installation of SAV for Windows NT/2000 and uses the **virus scanning** engine of the local Sophos Anti-Virus product to process all virus detection tasks. Users can start and stop the NWall processor and the Notes router from it. Antigen is more flexible than Sophos: it runs on all Notes versions from Notes 3.3 to Notes 5 and guards Notes mail servers based on IBM AIX, Solaris, and Windows NT 3.51 and 4.0 (Intel and Alpha). Three modules detect viruses (NScan, NShield, and NWall). Antigen, instead of using Sophos's 'dead message' method, **intercepts** and moves a tainted **document** into a temporary database.

COMPANY NAME: Sophos plc (629782); Sybari Software Inc (669679)
SPECIAL FEATURE: Screen Layouts Charts
DESCRIPTORS: File Security; Groupware; IBM PC & Compatibles; Network Software; Notes/Domino; System Monitoring; Windows NT/2000
REVISION DATE: 20030527

13/5/22 (Item 2 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2004 Info.Sources Inc. All rts. reserv.

00121741 DOCUMENT TYPE: Review

PRODUCT NAMES: Diskeeper Server for Windows 5.0 (783411)

TITLE: Dexterous Defragger: Executive Software Diskeeper 5.0 Server

AUTHOR: Norris, Jim
SOURCE: Windows NT Systems, v4 n1 p15(2) Jan 2000
ISSN: 1091-0212

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Executive Software's Diskeeper Server 5.0 is a Windows NT file system (NTFS) defragmenting utility. One of Diskeeper's best new features is the Frag Guard, which lessens or prevents fragmentation by **intercepting** and presorting **data** before it is written to disk. Diskeeper is effective and fast and guides the user as it is being run. Remote defragmentation is also trouble free and performs well even when utilities such as **virus scanners** are running on the remote system. Testing showed the system to be very stable, with no file corruptions or system crashes. If there is a crash or power outage, Diskeeper is also able to recover without losing data. Any problems that were found during testing were associated more with the nature of defragmentation rather than with Diskeeper.

File 347:JAPIO Nov 1976-2004/Mar(Updated 040708)

(c) 2004 JPO & JAPIO

File 350:Derwent WPIX 1963-2004/UD,UM &UP=200447

(c) 2004 Thomson Derwent

Set	Items	Description
S1	86648	VIRUS?? OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE?? OR WOR- M?? OR (MALICIOUS OR HOSTILE OR SUSPECT)() (LOGIC OR CODE OR S- OFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ? OR DATA OR INFORMATION OR PACKET? ?)
S2	13552	ANTIVIRUS OR ANTIVIRAL
S3	7578	S1(5N) (SCAN???? OR MONITOR??? OR CHECK??? OR INTERCEPT? OR PREVENT? OR IDENTIF? OR RECOGNI????? OR REMOV??? OR DELET??? OR ELIMINAT? OR ERAS??? OR ERADICAT??? OR FILTER???)
S4	1258	INTERCEPT???(7N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ? OR C- ONTENT OR DATA OR INFORMATION)
S5	17232	PORTAL? ? OR GATEWAY? ?
S6	0	S2:S3 AND S4 AND S5
S7	0	S1 AND S4 AND S5
S8	9	S1:S2 AND S4
S9	141	S1:S2 AND S5
S10	29	S8:S9 AND IC=G06F
S11	11	S10 AND AC=US/PR
S12	3	S11 AND AY=(1970:2000)/PR
S13	2	S10 AND PY=1970:2000
S14	5	S12:S13
S15	167	PA=ALADDIN?
S16	19	PA=TREND MICRO?
S17	186	S15:S16
S18	14	S1:S2 AND S17
S19	12	S18 AND AC=US/PR
S20	6	S19 AND AY=(1970:2000)/PR
S21	5	S18 AND PY=1970:2000
S22	10016	(UPLOADED OR CHECKED()IN OR INCOMING OR NEWLY()ARRIVED OR - NEW()ARRIVAL? ?) (5N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ? OR - DATA OR INFORMATION OR CONTENT)
S23	13	S1:S2 AND S22
S24	9	S23 AND AC=US/PR
S25	5	S24 AND AY=(1970:2000)/PR
S26	3	S23 AND PY=1970:2000
S27	6	S25:S26

14/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 2004 JPO & JAPIO. All rts. reserv.

06527278 **Image available**
PROPERTY BASE CONTEXT PORTAL

PUB. NO.: 2000-112999 [JP 2000112999 A]
PUBLISHED: April 21, 2000 (20000421)
INVENTOR(s): HIRSCH PETER DOUGLAS
APPLICANT(s): INFORMIX SOFTWARE INC
APPL. NO.: 11-279813 [JP 99279813]
FILED: August 25, 1999 (19990825)
PRIORITY: 139793 [US 98139793], US (United States of America), August
25, 1998 (19980825)
INTL CLASS: G06F-017/30 ; G06F-009/06

ABSTRACT

PROBLEM TO BE SOLVED: To attain the access of a user to the data through an information space called a scene by preparing a **worm** hole where a 2nd scene is projected from a 1st scene based on the 1st and 2nd zoom factors, etc.

SOLUTION: The primary parts of a user interface include a world manager window 10, a project work space 20, an editor window 22, an object inspector 30, a control bar 40 and an output window 24. Then a hyperlink system includes a 1st scene which has a 1st zoom factor covering a visual point through the 1st scene, a 2nd scene having a 2nd zoom factor that is nested in the 1st scene and has a 2nd zoom factor covering the 1st scene through the 2nd scene and a **worm** hole where the 1st scene is projected from the 2nd scene based on the 1st and 2nd zoom factors.

COPYRIGHT: (C)2000,JPO

14/5/2 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

016187412 **Image available**
WPI Acc No: 2004-345298/200432
XRPX Acc No: N04-275974

Encryption key escrow enforcing method for protected network, involves providing server, and detecting whether encryption key for decrypting data is stored in key escrow unit when detected data transmission includes encrypted data

Patent Assignee: CYBERSOFT INC (CYBE-N)

Inventor: RADATTI P V

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6721424	B1	20040413	US 99377311	A	19990819	200432 B

Priority Applications (No Type Date): US 99377311 A 19990819

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 6721424	B1	7	G06F-001/26	

Abstract (Basic): US 6721424 B1

NOVELTY - The method involves providing a server, and determining whether data transmission to a destination includes encrypted data. An encryption key for decrypting data stored in key escrow unit is determined if detected the data transmission includes the encrypted data. The data transmission to the destination is prevented unless an encryption key related with the destination is provided to the escrow unit.

DETAILED DESCRIPTION - A connection to an external source of data is monitored for an intended data transmission to the destination

within a protected network at a server.

USE - Used for enforcing encryption key escrow in a protected network (CLAIMED).

ADVANTAGE - The method provides a server with copies of the private encryption keys of the users of a protected network in such a manner that intervention of a network administrator is not required to ensure compliance with a key escrow policy.

DESCRIPTION OF DRAWING(S) - The drawing shows a functional block diagram of a local network connected via a proxy server to communicate with an external network.

External network (12)
User stations (14-16)
Local HUB (18)
Gateway server (20)
Virus database (22)
Hostage data storage (24)
pp; 7 DwgNo 1/3

Title Terms: ENCRYPTION; KEY; ESCROW; ENFORCE; METHOD; PROTECT; NETWORK; SERVE; DETECT; ENCRYPTION; KEY; DATA; STORAGE; KEY; ESCROW; UNIT; DETECT; DATA; TRANSMISSION; ENCRYPTION; DATA

Derwent Class: T01

International Patent Class (Main): G06F-001/26

File Segment: EPI

14/5/3 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

015594779 **Image available**

WPI Acc No: 2003-656934/200362

Related WPI Acc No: 2004-021110

XRPX Acc No: N03-523357

Data **protecting method for computer systems, involves intercepting write access command to location and comparing address of location to determine whether location is protected**

Patent Assignee: INASOFT INC (INAS-N)

Inventor: JIAN Z; SHEN A W; SUN H

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6594780	B1	20030715	US 99420348	A	19991019	200362 B

Priority Applications (No Type Date): US 99420348 A 19991019

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 6594780	B1	15	G06F-011/00	

Abstract (Basic): US 6594780 B1

NOVELTY - The method involves intercepting write access command to a location and comparing the address of the location to determine whether the location is protected. If the location is identified as protected then another location that is not protected is determined. The command that is re-directed to the latter location is sent to the former location to repeat the whole process until all the locations are protected.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a computer system for protecting the data residing in memory of computer systems.

USE - Used for protecting the data residing in memory of computer systems.

ADVANTAGE - The method provides security lock to the computing system to protect the operating system crash due to missing or corrupted files and **virus** penetration.

DESCRIPTION OF DRAWING(S) - The drawing shows a functional block diagram illustrating the data protecting method.

pp; 15 DwgNo 3/7

Title Terms: DATA; PROTECT; METHOD; COMPUTER; SYSTEM; INTERCEPT; WRITING;

ACCESS; COMMAND; LOCATE; COMPARE; ADDRESS; LOCATE; DETERMINE; LOCATE;
PROTECT

Derwent Class: T01
International Patent Class (Main): G06F-011/00
File Segment: EPI

14/5/4 (Item 3 from file: 350)
DIALOG(R) File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014395295 **Image available**
WPI Acc No: 2002-215998/200227
XRPX Acc No: N02-165502

**Anti- virus computer program file updating method using Internet,
involves sending e-mail message with header tag indicating availability
of updated anti- virus program file to user computer**

Patent Assignee: NETWORKS ASSOC TECHNOLOGY INC (NETW-N)

Inventor: BARTON C A; GARTSIDE P N; PINE K J

Number of Countries: 027 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020016959	A1	20020207	US 2000633358	A	20000804	200227 B
			US 2001944114	A	20010904	
EP 1288767	A2	20030305	EP 2002254593	A	20020628	200319

Priority Applications (No Type Date): US 2001944114 A 20010904; US
2000633358 A 20000804

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

US 20020016959 A1 14 G06F-009/445 CIP of application US 2000633358

EP 1288767 A2 E G06F-001/00

Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT
LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): US 20020016959 A1

NOVELTY - A header tag indicating the availability of the updated version of an anti- **virus** program file is embedded in an e-mail message, which is transmitted to a computer through a service provider. The computer automatically downloads the anti- **virus** program file from the FTP server (4), on reception of e-mail message.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) Anti- **virus** computer program file updating program;

(b) Anti- **virus** computer program file updating apparatus

USE - For updating anti- **virus** computer program file through Internet using proxy server, firewall, **gateway**, etc.

ADVANTAGE - Computers at a high risk to be affected by **viruses** can be immediately triggered, to download the updated computer file automatically, without requiring administrative intervention.

DESCRIPTION OF DRAWING(S) - The figure shows the anti- **virus** computer program file updating system.

FTP server (4)

pp; 14 DwgNo 1/9

Title Terms: ANTI; **VIRUS**; COMPUTER; PROGRAM; FILE; UPDATE; METHOD; SEND;
MAIL; MESSAGE; HEADER; TAG; INDICATE; AVAILABLE; UPDATE; ANTI; **VIRUS**;
PROGRAM; FILE; USER; COMPUTER

Derwent Class: T01

International Patent Class (Main): G06F-001/00 ; G06F-009/445

File Segment: EPI

14/5/5 (Item 4 from file: 350)
DIALOG(R) File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

013145373 **Image available**
WPI Acc No: 2000-317245/ 200027

XRPX Acc No: N00-238150

Gateway system for allowing limited communication between an external computing environment and an internal computing environment

Patent Assignee: PERFECTO TECHNOLOGIES LTD (PERF-N); SANCTUM LTD (SANC-N)

Inventor: RAANAN G; RESHEF E; SOLAN E

Number of Countries: 081 Number of Patents: 004

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200016206	A1	20000323	WO 98IL439	A	19980910	200027	B
AU 9890937	A	20000403	AU 9890937	A	19980910	200034	
			WO 98IL439	A	19980910		
EP 1118056	A1	20010725	EP 98942989	A	19980910	200143	
			WO 98IL439	A	19980910		
JP 2002533792	W	20021008	WO 98IL439	A	19980910	200281	
			JP 2000570676	A	19980910		

Priority Applications (No Type Date): WO 98IL439 A 19980910

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

WO 200016206 A1 E 64 G06F-013/38

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW

Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG ZW

AU 9890937 A G06F-013/38 Based on patent WO 200016206

EP 1118056 A1 E G06F-013/38 Based on patent WO 200016206

Designated States (Regional): AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

JP 2002533792 W 65 G06F-013/00 Based on patent WO 200016206

Abstract (Basic): WO 200016206 A1

NOVELTY - A communication channel enables the transfer of a simplified message between the first processor and a second processor. The first processor receives an external message, and converts the external message to the simplified message by mapping all or part of the external message content into a simplified representation of the content in accordance with a simplified protocol.

DETAILED DESCRIPTION - The second processor receives the simplified message transmitted by the first processor. The second processor converts the simplified message to an internal message by mapping the simplified representation of the content into an internal representation of the content in accordance with one or more internal environment protocols. INDEPENDENT CLAIMS are also included for the following:

- (a) a method for allowing limited communication between an external computing environment and an internal computing environment;
- (b) a system for allowing limited communication between an internal computing environment and an external computing environment;
- (c) a method for allowing limited communication between an internal computing environment and an external computing environment;
- (d) and a method for enabling formal verification of a system.

USE - For allowing limited communication between an external computing environment and an internal computing environment. Used for protecting trusted, internal networks from external attacks and intentional or inadvertent introduction of bugs or **viruses**.

ADVANTAGE - Limits communications between an external, untrusted environment and an internal trusted environment which effectively shields the internal environment from data potentially harmful to the internal environment. Allows a user to specify a set of simplified representations of content data which is allowed to pass from an external computing environment to an internal computing environment. Prevents any content data other than the specified data to pass to the internal environment by converting all allowable data into the simplified representations. Protects internal trusted computing environments from attacks from external computing environments.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of

the **gateway** system connected between an internal and external computing environment.

27/5/1 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014644578 **Image available**
WPI Acc No: 2002-465282/200250
XRPX Acc No: N02-366775

Web server has virus control mechanism that invokes virus checker application to check for virus in requested web page or e-mail message

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: BATES C L; DAY P R; SANTOSUOSSO J M
Number of Countries: 002 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
GB 2368163	A	20020424	GB 200114989	A	20010620	200250 B
KR 2002001651	A	20020109	KR 200137376	A	20010628	200250

Priority Applications (No Type Date): US 2000605258 A 20000911

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
GB 2368163	A	32	G06F-001/00	
KR 2002001651	A		G06F-015/16	

Abstract (Basic): GB 2368163 A

NOVELTY - A **virus** control mechanism invokes a **virus** checker application to check for a **virus** in requested web page or e-mail message. If the request information contains a **virus** , a web client is notified about the **virus** .

USE - Web server for providing information to web clients.

ADVANTAGE - Eliminates the need for installing **virus** checking software in web clients, since **virus** checker on a web server dynamically scans the **incoming data** when the server detects a **virus** , senders of **viruses** are notified, thus helping to inhibit proliferation of the **virus** .

DESCRIPTION OF DRAWING(S) - The figure shows a flow diagram of a method performed by the file **virus** processing mechanism.

pp; 32 DwgNo 8/12

Title Terms: WEB; SERVE; **VIRUS** ; CONTROL; MECHANISM; **VIRUS** ; CHECK; APPLY ; CHECK; **VIRUS** ; REQUEST; WEB; PAGE; MAIL; MESSAGE

Derwent Class: T01

International Patent Class (Main): G06F-001/00; G06F-015/16

File Segment: EPI

27/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX
(c) 2004 Thomson Derwent. All rts. reserv.

014213138 **Image available**
WPI Acc No: 2002-033835/200204
XRPX Acc No: N02-026055

Computer system for post-event reconstruction and security breach analysis on LAN, WAN, processes packet stream comprising data packets, to generate low level archival recording of network traffic

Patent Assignee: FALLON K T (FALL-I); JONES M R (JONE-I); TRCKA M V (TRCK-I); WALKER R W (WALK-I); DATADIRECT NETWORKS INC (DATA-N)

Inventor: FALLON K T; JONES M R; TRCKA M V; WALKER R W

Number of Countries: 001 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20010039579	A1	20011108	US 9630446	A	19961106	200204 B
			US 97852759	A	19970507	
US 6453345	B2	20020917	US 9630446	A	19961106	200264
			US 97852759	A	19970507	

Priority Applications (No Type Date): US 9630446 P 19961106; US 97852759 A 19970507

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes
US 20010039579 A1 34 G06F-015/173 Provisional application US 9630446

US 6453345 B2 G06F-015/173 Provisional application US 9630446

Abstract (Basic): US 20010039579 A1

NOVELTY - A network interface circuitry monitors the network and generates a packet stream comprising low data packets transmitted on the network by other computer systems. A computer processor processes the packet stream and generates an archival data stream which is recorded to a non-volatile data recorder for generating low level archival recording of network traffic.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

- (a) Network traffic archival record generating method;
- (b) Computer network traffic monitoring method;
- (c) Network firewall computer system operation evaluation method;
- (d) Non-network events monitoring system

USE - Used in internet connected computer networks such as LAN, WAN for facilitating post-event reconstruction and security breach analysis or other catastrophic event and for protecting network failures.

ADVANTAGE - By recording the archival data stream at the data link level, the **viruses** in the **incoming file** transfers are easily detected, the malicious acts that are performed on-site are detected and tracked and any type of network transactions such as e-mail communications and accesses to internal file server are virtually evaluated.

DESCRIPTION OF DRAWING(S) - The figure shows a flow diagram for illustrating a preferred process for passively generating a low level archival recording of network traffic.

pp; 34 DwgNo 1/19

Title Terms: COMPUTER; SYSTEM; POST; EVENT; RECONSTRUCT; SECURE; BREACH; ANALYSE; LAN; WAN; PROCESS; PACKET; STREAM; COMPRISE; DATA; PACKET; GENERATE; LOW; LEVEL; ARCHIVE; RECORD; NETWORK; TRAFFIC

Derwent Class: T01

International Patent Class (Main): G06F-015/173

International Patent Class (Additional): G06F-011/00

File Segment: EPI

27/5/3 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

014094961 **Image available**

WPI Acc No: 2001-579175/200165

XRPX Acc No: N01-431047

Virus checking method for multi server computer networks wherein the object or file is assigned metadata recording the operations performed

e.g. virus checking before forwarding to other servers

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)

Inventor: HAILPERN B T; MALKIN P K; PALMER C C; SCHLOSS R J; WHITE S R; YU P S

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6275937	B1	20010814	US 9764413	A	19971106	200165 B
			US 97979748	A	19971126	

Priority Applications (No Type Date): US 9764413 P 19971106; US 97979748 A 19971126

Patent Details:

Patent No Kind Lan Pg Main IPC Filing Notes

US 6275937 B1 27 G06F-007/00 Provisional application US 9764413

Abstract (Basic): US 6275937 B1

NOVELTY - The server receives a HTTP request from one of its clients, incorporated into this request is an instruction to perform a specific task before forwarding the file e.g. decryption etc.

Alternatively the server can perform default tasks on the file e.g. **virus** checking. Once the retrieval is complete, the server adds metadata tags to the file indicating tasks performed and the file forwarded to the user.

DETAILED DESCRIPTION - Alternatively the file could be forwarded to a different server to perform a different task e.g. Initial server attaches metadata tag and performs **virus** scan, then forwards the file to a different server for decryption and hence to the user.

An INDEPENDENT CLAIM is also included for a computer system and computer program using the method to **virus** check files across a multi-server network.

USE - To distribute routine tasks performed on **incoming files** from the Internet e.g. **virus** checking between server.

ADVANTAGE - As the metadata records the operations performed on the file e.g. time and date of **virus** check, program version etc, this record prevents the receiving server from duplicating operations, hence reducing server load.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of the server processes including the **virus** checking handler.

pp; 27 DwgNo 3/11

Title Terms: **VIRUS** ; CHECK; METHOD; MULTI; SERVE; COMPUTER; NETWORK; OBJECT; FILE; ASSIGN; RECORD; OPERATE; PERFORMANCE; **VIRUS** ; CHECK; FORWARDING; SERVE

Derwent Class: T01; W01

International Patent Class (Main): G06F-007/00

International Patent Class (Additional): H04L-009/00

File Segment: EPI

27/5/4 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

012964674 **Image available**

WPI Acc No: 2000-136525/ 200012

Related WPI Acc No: 1995-215329; 2000-051976; 2000-222194; 2001-482748; 2001-578394; 2004-050944

XRPX Acc No: N00-102098

Incoming telephone call routing and handling method in confidential medical testing system for human immunodeficiency virus

Patent Assignee: HOME ACCESS HEALTH CORP (HOME-N)

Inventor: QUATTROCCHI R A

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 6016345	A	20000118	US 93146307	A	19931102	200012 B
			US 95420694	A	19950412	
			US 97822166	A	19970321	

Priority Applications (No Type Date): US 95420694 A 19950412; US 93146307 A 19931102; US 97822166 A 19970321

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6016345	A		15	H04M-003/00	CIP of application US 93146307 Cont of application US 95420694

Abstract (Basic): US 6016345 A

NOVELTY - After the receipt of a telephone call initiated by an anonymous caller, the caller is prompted to transmit a personal ID code corresponding to a specimen submitted already to a medical laboratory for analysis. A test result associated with the received personal ID code is retrieved and routed through a selected call handler, to the anonymous caller.

DETAILED DESCRIPTION - The call handler is selected with respect to the retrieved test result **information** to process the **incoming** telephone call. An INDEPENDENT CLAIM is also included for an incoming telephone call routing and handling system.

USE - In confidential medical testing system for human

immunodeficiency **virus** (HIV).

ADVANTAGE - Enables to conduct test confidentially without having to reveal the identity of a person. Enables a person to undertake a test anonymously and to obtain test result confidentially.

DESCRIPTION OF DRAWING(S) - The figure shows block diagram of telephone call routing and handling system.

pp; 15 DwgNo 6/8

Title Terms: INCOMING; TELEPHONE; CALL; ROUTE; HANDLE; METHOD; CONFIDE; MEDICAL; TEST; SYSTEM; HUMAN; IMMUNODEFICIENCY; **VIRUS**

Derwent Class: S05; W01

International Patent Class (Main): H04M-003/00

File Segment: EPI

27/5/5 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

010369387 **Image available**

WPI Acc No: 1995-270749/ 199536

XRPX Acc No: N95-208315

Digital data communication apparatus with antivirus system - has receiver with antivirus module within temporary data store for recognition and extraction of virus before passing data to main processor

Patent Assignee: DASSAULT AUTOMATISMES & TELECOM (AVIO)

Inventor: BASSET J

Number of Countries: 017 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
EP 666671	A1	19950809	EP 95400161	A	19950125	199536 B
FR 2715788	A1	19950804	FR 941091	A	19940201	199536

Priority Applications (No Type Date): FR 941091 A 19940201

Cited Patents: 2.Jnl.Ref; WO 9322723

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
-----------	------	-----	----	----------	--------------

EP 666671	A1	F	7	H04L-029/06	
-----------	----	---	---	-------------	--

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

FR 2715788	A1			H04L-029/06	
------------	----	--	--	-------------	--

Abstract (Basic): EP 666671 A

The apparatus includes a transmitter (1) and a receiver (2). Each includes a processor (10,20) with a hard disk (12,22) and a communications interface (15,25). The interfaces communicate across the digital access network (RN) with both parts containing communications modules with a predetermined protocol for transfer to disk.

The receiver has a temporary memory store (26) which is used to communicate with the processor. An anti- **virus** module (220) within the temporary store contains information on **viruses** , for comparison with the **incoming data** and extraction of the uncontaminated data.

ADVANTAGE-Removes computer **viruses** before reception, preventing infection of computer. Anti- **virus** module can be updated for new **viruses** .

Dwg.2/3

Title Terms: DIGITAL; DATA; COMMUNICATE; APPARATUS; **ANTIVIRAL** ; SYSTEM; RECEIVE; **ANTIVIRAL** ; MODULE; TEMPORARY; DATA; STORAGE; RECOGNISE; EXTRACT; **VIRUS** ; PASS; DATA; MAIN; PROCESSOR

Derwent Class: T01; W01

International Patent Class (Main): H04L-029/06

File Segment: EPI

27/5/6 (Item 6 from file: 350)

DIALOG(R)File 350:Derwent WPIX

(c) 2004 Thomson Derwent. All rts. reserv.

009915268 **Image available**

WPI Acc No: 1994-182978/ 199422

XRPX Acc No: N94-144546

In transit detection of computer virus with safeguard - testing each character of incoming data stream using finite state machine and preventing data remaining on destination storage medium when virus detected

Patent Assignee: HILGRAEVE CORP (HILG-N)

Inventor: GRAY M H; HILE J K; WAKELIN D L

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 5319776	A	19940607	US 90511218	A	19900419	199422 B
			US 92954784	A	19920929	

Priority Applications (No Type Date): US 90511218 A 19900419; US 92954784 A 19920929

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
US 5319776	A	15	H04L-009/00	Cont of application US 90511218

Abstract (Basic): US 5319776 A

The **virus** detection method involves causing a quantity of digital data resident on a source storage medium to be transferred to a computer system having a destination storage medium. The transferred digital data is received and screened prior to storage on the destination storage medium to determine if at least one predefined sequences are present in the digital data received. In response to the screening step the screened digital data is automatically stored on the destination storage medium if none of the predefined sequences are present.

The screened digital data is automatically inhibited from being stored on the destination storage medium if at least one predefined sequence is present. Preferably at least one predefined sequence is based upon a computer **virus** signature. The screening is performed using at least one finite state table.

USE/ADVANTAGE - Checks data before storage therefore reducing risk of disc corruption.

File 348:EUROPEAN PATENTS 1978-2004/Jul W02

(c) 2004 European Patent Office

File 349:PCT FULLTEXT 1979-2002/UB=20040722,UT=20040715

(c) 2004 WIPO/Univentio

Set	Items	Description
S1	104779	VIRUS?? OR VIRAL OR MACROVIRUS?? OR TROJAN()HORSE?? OR WOR- M?? OR (MALICIOUS OR HOSTILE OR SUSPECT) () (LOGIC OR CODE OR S- OFTWARE OR PROGRAM?? OR ALGORITHM? ? OR COMMAND? ? OR SIGNAL? ? OR INSTRUCTION? ? OR DATA OR INFORMATION OR PACKET? ?)
S2	17046	ANTIVIRUS OR ANTIVIRAL
S3	18076	S1(5N) (SCAN???? OR MONITOR??? OR CHECK??? OR INTERCEPT? OR PREVENT? OR IDENTIF? OR RECOGNI????? OR REMOV??? OR DELET??? OR ELIMINAT? OR ERAS??? OR ERADICAT??? OR FILTER????)
S4	3700	INTERCEPT??? (7N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ? OR C- ONTENT OR DATA OR INFORMATION)
S5	30839	PORTAL? ? OR GATEWAY? ?
S6	5517	S1(5N) (IDENTIF???? OR IDENTIFICATION)
S7	1	(S3 OR S6) (50N) S4 (50N) (S5 OR PROXY()SERVER? ?)
S8	2567	PROXY()SERVER? ?
S9	3	S1(50N) S4 (50N) (S5 OR S8)
S10	24	(S3 OR S6) (50N) S4
S11	117	(S3 OR S6) (50N) (S5 OR S8)
S12	141	S7 OR S9:S11
S13	90	S12 AND IC=G06F
S14	68	S13 AND AC=US/PR
S15	52	S14 AND AY=(1970:2000)/PR
S16	16	S13 AND PY=1970:2000
S17	53	S15:S16
S18	53	S1:S2(50N) S4
S19	23	S18 NOT S12
S20	13	S19 AND AC=US/PR
S21	5	S20 AND AY=(1970:2000)/PR
S22	7	S19 AND PY=1970:2000
S23	7	S21:S22
S24	2193	(UPLOADED OR CHECKED() IN OR INCOMING OR NEWLY()ARRIVED OR - NEW()ARRIVAL? ?) (5N) (DOCUMENT? ? OR ARTICLE? ? OR FILE? ?)
S25	21	S1(30N) S24
S26	17	S25 NOT S12
S27	169	S1:S2(50N) INTERCEPT?
S28	81	S27 AND IC=G06F
S29	42	S28 NOT (S12 OR S23 OR S26)
S30	27	S29 AND AC=US/PR
S31	16	S30 AND AY=(1970:2000)/PR
S32	11	S29 AND PY=1970:2000
S33	21	S31:S32

17/3,K/5 (Item 5 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00943106

ANTI-VIRUS AGENT FOR USE WITH DATABASES AND MAIL SERVERS
ANIT-VIRUS-AGENT ZUR VERWENDUNG MIT DATENBANKEN UND POSTSERVER
AGENT ANTI-VIRUS DESTINE A ETRE UTILISE AVEC DES BASES DE DONNEES ET DES
SERVEURS DE MESSAGERIES

PATENT ASSIGNEE:

Computer Associates Think, Inc., (2947530), One Computer Associates Plaza
, Islandia, New York 11749, (US), (Proprietor designated states: all)

INVENTOR:

CHEN, Chia-Hwang, 19 Elaine Place, Plainview, NY 11803, (US)

LUO, Chih-Ken, 31 Lauren Avenue, Dix Hills, NY 11746, (US)

LEGAL REPRESENTATIVE:

Cross, Rupert Edward Blount et al (42891), BOULT WADE TENNANT, Verulam
Gardens 70 Gray's Inn Road, London WC1X 8BT, (GB)

PATENT (CC, No, Kind, Date): EP 1010059 A2 000621 (Basic)
EP 1010059 B1 030521
WO 98010342 980312

APPLICATION (CC, No, Date): EP 97940851 970905; WO 97US15661 970905

PRIORITY (CC, No, Date): US 709025 960905

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU;
MC; NL; PT; SE

RELATED DIVISIONAL NUMBER(S) - PN (AN):

EP 1237065 (EP 2002077028)

INTERNATIONAL PATENT CLASS: **G06F-007/02** ; **G06F-011/00** ; H04L-009/00

NOTE:

No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200321	866
CLAIMS B	(German)	200321	807
CLAIMS B	(French)	200321	1155
SPEC B	(English)	200321	6309
Total word count - document A			0
Total word count - document B			9137
Total word count - documents A + B			9137

INTERNATIONAL PATENT CLASS: **G06F-007/02** ...

... **G06F-011/00**

...SPECIFICATION received internally never reach the proxy post office and so are never scanned. Accordingly, users may transmit viruses via e-mail internally within the organization. **ScanMail** is incapable of detecting **viruses** in e-mail attachments that originate within and stay within a LAN.

Another product that purports to scan for attachments to e-mail is InterScan VirusWall (RTM) distributed by Trend Micro Devices, Inc.. When installed on a UNIX Internet **gateway**, InterScan **Virus** Wall (RTM) is intended to **intercept** and scan e-mail attachments, FTP transfers, World Wide Web downloads and uploads and transfers of data between in-house PCS or LANs and the outside world. InterScan VirusWall (RTM) consists of an FTP **proxy server** for **gateway** traffic and a Simple Mail Transfer Protocol (SMTP) **proxy server** for e-mail. As with the ScanMail application, the InterScan VirusWall (RTM) program is only capable of scanning e-mail attachments that pass through the on the **gateway** and scans individual packets, it may not be sufficiently efficient to detect polymorphic viruses or compressed files if the files are larger then one packet size on the network.

A product called Antigen (RTM) distributed by Sybari transfers e-mail attachments to a third party **virus scanner** for detection of **virus**. However, Antigen (RTM) is incapable of reattaching the e-mail attachment back to the e-mail message if a virus is discovered and cured. Although ...capable of processing e-mail messages that originate within LAN 100

(including Intranet e-mail messages) or that enter LAN 100 from the Internet through **gateway** 40 (Internet e-mail messages).

The InocuLAN program 120 will alert specified individuals via the e-mail system or via Cheyenne Software, Inc.'s Alert Generic Notification system to warn users so as to stop the **virus** from spreading. The InocuLAN Local **Scanner** and Job Service work conjunctively with the agent 110 to perform virus scanning and curing within the message system and to ensure a virus free...

- ...CLAIMS received at the message system (130) within the previous scan time period;
- means for passing each attachment in the list of attachments to the anti- **virus** system (120) for computer **virus scanning**; and
 - means for re-attaching each attachment to the e-mail messages.
10. The system of claim 9 wherein the e-mail messages comprises e-mail messages received from client computers (10, 30) on the computer network.
 11. The system of claim 10 wherein the message system comprises an external **gateway** (40) and the e-mail messages comprise e-mail messages received from external message systems.
 12. The system of claim 9 wherein the e-mail messages comprise e-mail messages received over an Internet connection.
 13. A real-time system for detecting and **removing** computer **viruses** located in attachments to e-mail messages in a client-server computer network including a server computer (20), a plurality of client computers (10, 30...

17/3,K/6 (Item 6 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

00934787

Secure two-piece user authentication in a computer network
Gesicherte zweiteilige Benutzer-Authentifizierung in einem Rechnernetz
Authentification en deux pieces securisee d'un utilisateur dans un reseau d'ordinateurs

PATENT ASSIGNEE:

Compaq Computer Corporation, (687792), 20555 S.H. 249, Houston Texas 77070, (US), (Proprietor designated states: all)

INVENTOR:

Angelo, Michael F., 14926 Walters Road, Houston, Texas 77068, (US)
Olarig, Sompong P., 15415 Evergreen Knoll Lane, Cypress, Texas 77429, (US)

LEGAL REPRESENTATIVE:

Brunner, Michael John et al (28871), GILL JENNINGS & EVERY, Broadgate House, 7 Eldon Street, London EC2M 7LH, (GB)

PATENT (CC, No, Kind, Date): EP 851335 A2 980701 (Basic)

EP 851335 A3 990616

EP 851335 B1 031029

APPLICATION (CC, No, Date): EP 97310653 971230;

PRIORITY (CC, No, Date): US 774809 961231

DESIGNATED STATES: DE; FR; GB

INTERNATIONAL PATENT CLASS: **G06F-001/00**

ABSTRACT WORD COUNT: 306

NOTE:

Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	199827	840
CLAIMS B	(English)	200344	935
CLAIMS B	(German)	200344	878
CLAIMS B	(French)	200344	1187
SPEC A	(English)	199827	6236
SPEC B	(English)	200344	6406
Total word count - document A			7077

Total word count - document B 9406
Total word count - documents A + B 16483

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION 657982. Briefly, a request for secure keyboard communications causes the computer's processor to enter into SMM. The SMI handler then directs specialized hardware to **intercept** and divert keyboard interrupts, such that **data** entered via the keyboard is only communicated to secure, non-readable memory. The secured keyboard communications channel prevents the user's plain text password from being **intercepted** by **malicious software** code, such as a virus masquerading as a screen saver or device driver.

Thus, a method has been described for permitting secure user authentication and...

...SPECIFICATION 657982. Briefly, a request for secure keyboard communications causes the computer's processor to enter into SMM. The SMI handler then directs specialized hardware to **intercept** and divert keyboard interrupts, such that **data** entered via the keyboard is only communicated to secure, non-readable memory. The secured keyboard communications channel prevents the user's plain text password from being **intercepted** by **malicious software** code, such as a virus masquerading as a screen saver or device driver.

Thus, a method has been described for permitting secure user authentication and...

17/3,K/7 (Item 7 from file: 348)
DIALOG(R) File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00662890

Method and apparatus for detection of computer viruses
Verfahren und Gerat zur Erkennung von Computerviren
Procede et appareil de detection de virus d'ordinateurs
PATENT ASSIGNEE:

Chambers, David Alan, (1817400), 3655 Eastwood Circle, Santa Clara,
California 95054, (US), (Proprietor designated states: all)

INVENTOR:

Chambers, David Alan, 3655 Eastwood Circle, Santa Clara, California 95054
, (US)

LEGAL REPRESENTATIVE:

O'Connell, David Christopher et al (62551), Haseltine Lake & Co.,
Imperial House, 15-19 Kingsway, London WC2B 6UD, (GB)

PATENT (CC, No, Kind, Date): EP 636977 A2 950201 (Basic)
EP 636977 A3 970806
EP 636977 B1 010523

APPLICATION (CC, No, Date): EP 94305551 940727;

PRIORITY (CC, No, Date): US 99368 930729

DESIGNATED STATES: BE; DE; FR; GB; IT

INTERNATIONAL PATENT CLASS: **G06F-011/00**

ABSTRACT WORD COUNT: 114

NOTE:

Figure number on first page: 1B

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	464
CLAIMS B	(English)	200121	593
CLAIMS B	(German)	200121	525
CLAIMS B	(French)	200121	665
SPEC A	(English)	EPABF2	5575
SPEC B	(English)	200121	5666
Total word count - document A			6040
Total word count - document B			7449
Total word count - documents A + B			13489

...SPECIFICATION programs can be generally categorized into groups:
behavior interceptors, signature scanners, and checksum monitors.

BEHAVIOR INTERCEPTORS

The earliest antivirus programs were generally of the behavior **interceptor** type: they would allow a **virus** program to execute in memory but would intercept strategic operating system function requests made by the computer virus. Such requests would generally be functions which the virus required to be performed in order to replicate or to destroy its host, i.e., "Write to a file", "Erase a **file** ", "Format a disk" etc. By **intercepting** these requests, the computer operator/user could be informed that a potentially dangerous function was about to be performed. Control could be halted or continued as necessary. Some antivirus programs actually modify the instructions of the discovered virus program and make them inoperable so as to "kill" them.

The behavior **interceptor** method of **virus** detection has several drawbacks. The first problem is that it relies entirely on user input and decision making when potentially dangerous behavior is detected. This...

...SPECIFICATION programs can be generally categorized into groups:
behavior interceptors, signature scanners, and checksum monitors.

BEHAVIOR INTERCEPTORS

The earliest antivirus programs were generally of the behavior **interceptor** type: they would allow a **virus** program to execute in memory but would intercept strategic operating system function requests made by the computer virus. Such requests would generally be functions which the virus required to be performed in order to replicate or to destroy its host, i.e., "Write to a file", "Erase a **file** ", "Format a disk" etc. By **intercepting** these requests, the computer operator/user could be informed that a potentially dangerous function was about to be performed. Control could be halted or continued as necessary. Some antivirus programs actually modify the instructions of the discovered virus program and make them inoperable so as to "kill" them.

The behavior **interceptor** method of **virus** detection has several drawbacks. The first problem is that it relies entirely on user input and decision making when potentially dangerous behavior is detected. This...

33/3,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

01446197

Method and system for creating and maintaining version-specific properties
in a distributed environment
Verfahren und Vorrichtung zur Erzeugung und Erhaltung von
versionsspezifischen Eigenschaften in einer Datei
Procede et dispositif pour creer et maintenir des proprietes specifiques de
version dans un fichier

PATENT ASSIGNEE:

MICROSOFT CORPORATION, (749861), One Microsoft Way, Redmond, Washington
98052-6399, (US), (Applicant designated States: all)

INVENTOR:

Goldick, Jonathan S., 565A Natoma Street, San Francisco, California 94103
, (US)

LEGAL REPRESENTATIVE:

Grunecker, Kinkeldey, Stockmair & Schwanhauser Anwaltssozietat (100721)
, Maximilianstrasse 58, 80538 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 1237073 A2 020904 (Basic)

APPLICATION (CC, No, Date): EP 2001130445 011220;

PRIORITY (CC, No, Date): US 750501 001227

DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI;
LU; MC; NL; PT; SE; TR

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: G06F-009/44

ABSTRACT WORD COUNT: 73

NOTE:

Figure number on first page: 2

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200236	793
SPEC A	(English)	200236	6544
Total word count - document A			7337
Total word count - document B			0
Total word count - documents A + B			7337

INTERNATIONAL PATENT CLASS: G06F-009/44

...SPECIFICATION resources), among others.

Often, third party applications work in combination with a server-side resource systems to provide additional system features or functions, such as **virus** scanning functions. These third party applications may actually " **intercept** " each resource access attempt and scan the object for **viruses** or perform other tests prior to performing the actual access operation. Unfortunately however, performing a scan operation or other tests each time a resource is...

33/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS
(c) 2004 European Patent Office. All rts. reserv.

00993581

Method for securely communicating remote control commands in a computer
network
Verfahren zur gesicherten Kommunikation von Fernbedien-Befehlen in einem
Rechnernetz
Procede de communication securisee de telecommandes dans un reseau
d'ordinateurs

PATENT ASSIGNEE:

Compaq Computer Corporation, (687792), 20555 S.H. 249, Houston Texas
77070, (US), (Applicant designated States: all)

INVENTOR:

Angelo, Michel F., 14926 Walters Road, Houston, Texas 77068, (US)

Collins, David L., 28506 Champion Oaks, Magnolia, Texas 77354, (US)
Kim, Donald D., 12902 Orchard Hollow Way, Houston, Texas 77065, (US)
Jansen, Kenneth A., 17319 Thorhill, Spring, Texas 77379, (US)

LEGAL REPRESENTATIVE:

Brunner, Michael John et al (28871), GILL JENNINGS & EVERY Broadgate
House 7 Eldon Street, London EC2M 7LH, (GB)

PATENT (CC, No, Kind, Date): EP 898216 A2 990224 (Basic)
EP 898216 A3 000223

APPLICATION (CC, No, Date): EP 98306483 980814;

PRIORITY (CC, No, Date): US 916273 970822

DESIGNATED STATES: DE; FR; GB

EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI

INTERNATIONAL PATENT CLASS: **G06F-001/00**

ABSTRACT WORD COUNT: 206

NOTE:

Figure number on first page: 3

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9907	1020
SPEC A	(English)	9907	5211
Total word count - document A			6231
Total word count - document B			0
Total word count - documents A + B			6231

INTERNATIONAL PATENT CLASS: **G06F-001/00**

...SPECIFICATION algorithms. The encryption processes are preferably carried out in secure memory that is not readable or writeable and cannot be "sniffed" by surreptitious programs or **viruses** having the ability to monitor and **intercept** processes running in normal memory. Such a memory configuration is disclosed, for example, in "METHOD FOR SECURELY CREATING, STORING AND USING ENCRYPTION KEYS IN A...

33/3,K/3 (Item 3 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

00935205

ISOLATED EXECUTION LOCATION

ISOLIERTER AUSFUHRUNGSORT

LIEU ISOLE D'EXECUTION

PATENT ASSIGNEE:

Citrix Systems (Research and Development) Limited, (2669040), Buckingham
Court Kingsmead Business Park London Road, High Wycombe Buckinghamshire
HP11 1JU, (GB), (Proprietor designated states: all)

INVENTOR:

BULL, John Albert, The Almshouses, Great Brington, NNNorthants NN7 4HY,
(GB)

OTWAY, David John, 12 Willis Road, Cambridge CB1 2AQ, (GB)

KRAMER, Andre, 16 Clare Street, Cambridge CB3 4BJ, (GB)

LEGAL REPRESENTATIVE:

Dummett, Thomas Ian Peter et al (30313), Dummett Copp & Co. 25 The Square
, Martlesham Heath, Ipswich, Suffolk IP5 7SL, (GB)

PATENT (CC, No, Kind, Date): EP 978036 A1 000209 (Basic)
EP 978036 B1 011121
WO 9808163 980226

APPLICATION (CC, No, Date): EP 97932960 970807; WO 97IB973 970807

PRIORITY (CC, No, Date): GB 9616783 960809; GB 9703773 970224

DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GR; IE; IT; LI; NL; PT;
SE

INTERNATIONAL PATENT CLASS: **G06F-009/46 ; G06F-001/00**

NOTE:

No A-document published by EPO

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200147	1364
CLAIMS B	(German)	200147	1127
CLAIMS B	(French)	200147	1433
SPEC B	(English)	200147	9021
Total word count - document A			0
Total word count - document B			12945
Total word count - documents A + B			12945

INTERNATIONAL PATENT CLASS: **G06F-009/46** ...

... **G06F-001/00**

...SPECIFICATION be used to inspect and verify incoming program components which it is desired to download into the end user system and can be used to **intercept virus** programs before they reach the end user system. Whilst the end user may be confident that specified program components are acceptable, in which case he...

33/3,K/4 (Item 4 from file: 348)

DIALOG(R)File 348:EUROPEAN PATENTS

(c) 2004 European Patent Office. All rts. reserv.

00552076

Authentication method and system with a smartcard.

Verfahren und System zur Authentifizierung mit einer Chipkarte.

Methode et systeme d'authentification a l'aide d'une carte a puce.

PATENT ASSIGNEE:

International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB)

INVENTOR:

Molva, Refik, Dr., Villa Koubagne, 8 Impasse Des Oliviers, F-06160

Juan-Les-Pins, (FR)

Tsudik, Gene, Dr., Auf der Mauer 3, CH-8800 Thalwil, (CH)

LEGAL REPRESENTATIVE:

Barth, Carl Otto et al (1411), IBM Corporation Saumerstrasse 4, CH-8803

Ruschlikon, (CH)

PATENT (CC, No, Kind, Date): EP 566811 A1 931027 (Basic)

APPLICATION (CC, No, Date): EP 92810294 920423;

PRIORITY (CC, No, Date): EP 92810294 920423

DESIGNATED STATES: DE; FR; GB

INTERNATIONAL PATENT CLASS: **G06F-001/00** ; G07F-007/10

ABSTRACT WORD COUNT: 101

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1183
SPEC A	(English)	EPABF1	5824
Total word count - document A			7007
Total word count - document B			0
Total word count - documents A + B			7007

INTERNATIONAL PATENT CLASS: **G06F-001/00** ...

...SPECIFICATION smartcard can be stolen.

Any public work station can be taken over by a hostile party. All communication involving a work station is subject to **interception** and divulgement and the work station may contain **trojan horse** programs that disclose all the information entered by the user into the work station or sent by the AS.

A bona fide registered user may...

33/3,K/5 (Item 1 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00961470 **Image available**

**DECENTRALIZED VIRUS SCANNING FOR STORED DATA
RECHERCHE DECENTRALISEE DE VIRUS POUR DONNEES STOCKEES**

Patent Applicant/Assignee:

NETWORK APPLIANCE INC, 495 East Java Drive, Sunnyvale, CA 94089, US, US
(Residence), US (Nationality)

Inventor(s):

MUHLESTEIN Mark, 5831 E. Placita Alta Reposa, Tucson, AZ 85750, US,

Legal Representative:

SWERNOFSKY Steven A (agent), Swernofsky Law Group, P.O. Box 390013,
Mountain View, CA 94039-0013, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200295588 A2-A3 20021128 (WO 0295588)

Application: WO 2001US51581 20011130 (PCT/WO US0151581)

Priority Application: US 2000728701 20001201

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

CA JP

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

Publication Language: English

Filing Language: English

Fulltext Word Count: 7736

Main International Patent Class: **G06F-011/30**

Fulltext Availability:

Detailed Description

Detailed Description

... expense.

A second known method for protecting against computer viruses is to have the end user run anti-virus software on their client device. Anti-**virus** software packages are offered by such companies as McAfee and Syrnantec. These programs are loaded during the boot stage of a computer and work as a background job monitoring memory and files as they are opened and saved.

While this second known method is effective at **intercepting** and protecting the client device from infection, it suffers from several drawbacks. It places the burden of detection at the last possible link in the chain. If for any reason the **virus** is not detected prior to reaching the end user it is now at the computing device where it will do the most damage (corrupting files...

33/3,K/6 (Item 2 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00910741 **Image available**

**DECENTRALIZED APPLIANCE VIRUS SCANNING
DETECTION DE VIRUS DECENTRALISEE POUR APPAREILS**

Patent Applicant/Assignee:

NETWORK APPLIANCE INC, 495 East Java Drive, Sunnyvale, CA 94089, US, US
(Residence), US (Nationality)

Inventor(s):

MUHLESTEIN Mark, 5831 E. Placita Alta Reposa, Tucson, AZ 85750, US,

Legal Representative:

SWERNOFSKY Steven A (agent), Swernofsky Law Group, P.O. Box 390013,
Mountain View, CA 94039-0013, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200244862 A2-A3 20020606 (WO 0244862)

Application: WO 2001US46688 20011130 (PCT/WO US0146688)

Priority Application: US 2000728701 20001201

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

CA JP

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

Publication Language: English

Filing Language: English

Fulltext Word Count: 6007

Main International Patent Class: **G06F-007/00**

International Patent Class: **G06F-011/34**

Fulltext Availability:

Detailed Description

Detailed Description

... expense.

A second known method for protecting against computer viruses is to have the end user run anti-virus software on their client device. Anti-**virus** software packages are offered by such companies as McAfee and Symantec. These programs are loaded during the boot stage of a computer and work as a background job monitoring memory and files as they are opened and saved.

While this second known method is effective at **intercepting** and protecting the client device from infection, it suffers from several drawbacks. It places the burden of detection at the last possible link in the chain. If for any reason the **virus** is not detected prior to reaching the end user it is now at the computing device where it will do the most damage (corrupting files...

33/3,K/7 (Item 3 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00901268 **Image available**

ANALYTICAL VIRTUAL MACHINE

MACHINE VIRTUELLE ANALYTIQUE

Patent Applicant/Assignee:

VCIS INC, 522 Erskine Drive, Pacific Palisades, CA 90272, US, US

(Residence), US (Nationality)

Inventor(s):

VAN DER MADE Peter A J, 201 Barrenjoey Rd., Newport Beach, NSW 2106, AU,

Legal Representative:

WRIGHT William H (et al) (agent), Hogan & Hartson L.L.P., Biltmore Tower, Suite 1900, 500 South Grand Avenue, Los Angeles, CA 90071, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200235328 A1 20020502 (WO 0235328)

Application: WO 2001US26804 20010828 (PCT/WO US0126804)

Priority Application: US 2000242939 20001024; US 2001885427 20010619

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 6457

Main International Patent Class: **G06F-001/00**

Fulltext Availability:

Detailed Description

Detailed Description

... program file is detected by a variation in the CRC value. Checksum monitors improve on integrity check systems in that it is more difficult for **malicious code** to defeat the monitoring. On the other hand, checksum monitors exhibit the same limitations as integrity checking systems in that many false warnings issue and it is difficult to identify which warnings represent actual **viruses** or infection. Behavior **interception** systems detect **virus** activity by interacting with the operating system of the target computer and monitoring for potentially malicious behavior. When such malicious behavior is detected, the action is blocked and the user is informed that a potentially dangerous action is about to take place. The potentially **malicious code** can be allowed to perform this action by the user. This makes the behavior **interception** system somewhat unreliable, because the effectiveness of the system depends on user input. In addition, resident behavior **interception** systems are sometimes detected and disabled by **malicious code**.

Another conventional strategy for detecting infections is the use of bait files. This strategy is typically used in combination with other **virus** detection strategies to detect an existing and active infection. This means that the **malicious code** is presently running on the target computer and is modifying files. The virus is detected when the bait file is modified. Many viruses are aware...

33/3,K/8 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00893315 **Image available**

WRITE PROTECTION FOR COMPUTER LONG-TERM MEMORY DEVICES
PROTECTION CONTRE L'ECRIURE POUR DISPOSITIFS A MEMOIRE A LONG TERME
D'ORDINATEUR

Patent Applicant/Inventor:

BRESS Steven, 9801-C Gable Ridge Terrace, Rockville, MD 20850, US, US
(Residence), US (Nationality)

MENZ Mark Joseph, 114 Rawlings Court, Folsom, CA 95630, US, US
(Residence), US (Nationality)

Legal Representative:

LEDELL Brian E (agent), Harrity & Snyder, L.L.P., 11240 Waples Mill Road,
Suite 300, Fairfax, VA 22030, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200227445 A2-A3 20020404 (WO 0227445)

Application: WO 2001US30502 20010928 (PCT/WO US0130502)

Priority Application: US 2000237761 20000929

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK
SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 9235

Main International Patent Class: **G06F-001/00**

Fulltext Availability:

Detailed Description

Detailed Description

... and a logic circuit connects the emulator component to the interface and is configured to compare information received at the emulator component to a computer **virus** definition file and to block transmission of storage commands from the emulator component to the interface when the comparison indicates a match with the computer **virus** definition file.

Another aspect of the invention is a method that **intercepts** communications between a computer motherboard and a local storage device and compares commands in the communications between the motherboard and the storage device to a...

33/3,K/9 (Item 5 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00883044 **Image available**

**METHOD AND SYSTEM FOR SHARING BIOLOGICAL INFORMATION
PROCEDE ET SYSTEME DE PARTAGE D'INFORMATIONS BIOLOGIQUES**

Patent Applicant/Assignee:

VARRO TECHNOLOGIES INC, 325 Cherry Street, 1st floor, Philadelphia, PA 19106, US, US (Residence), US (Nationality)

Inventor(s):

HEDGEPTH Chester III, 2300 Walnut Street, Apt. 727, Philadelphia, PA 19103, US,

SHIN David Sullivan, 318 Lincoln Woods, Lafayette Hill, PA 19444, US,

VENKATESAN Jay Raman, 514 South 22nd Street, Philadelphia, PA 19146, US,

Legal Representative:

GOLUB Daniel H (agent), 1701 Market Street, Philadelphia, PA 19103, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200217190 A1 20020228 (WO 0217190)

Application: WO 2001US25956 20010820 (PCT/WO US0125956)

Priority Application: US 2000643643 20000822

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 12571

Main International Patent Class: **G06F-017/60**

Fulltext Availability:

Detailed Description

Detailed Description

... each member.

The software further comprises features for enhancing the security of individual members associated with the network. The software in one embodiment includes a **virus** scanner which determines whether biological information made available for sharing is

4

infected with a computer **virus**, and if infected reports the infection to the network host.

In another embodiment, the software encrypts the biological information being transferred so that it may not be **intercepted** during transmission. In an alternate embodiment, digital rights management technologies are used to limit the use of the biological information by the searching member who...

33/3,K/10 (Item 6 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00872831 **Image available**

COMPUTER IMMUNE SYSTEM AND METHOD FOR DETECTING UNWANTED CODE IN A COMPUTER SYSTEM

SYSTEME INFORMATIQUE IMMUNISE DETECTANT LES CODES INDESIRABLES DANS UN SYSTEME INFORMATIQUE

Patent Applicant/Assignee:

VCIS INC, 522 Erskine Drive, Pacific Palisades, CA 90272, US, US
(Residence), US (Nationality)

Inventor(s):

VAN DER MADE Peter A J, 17 Nooal Street, Newport Beach, NSW 2106, AU,

Legal Representative:

WRIGHT William H (et al) (agent), Hogan & Hartson L.L.P., Biltmore Tower, Suite 1900, 500 South Grand Avenue, Los Angeles, CA 90071, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200206928 A2-A3 20020124 (WO 0206928)

Application: WO 2001US19142 20010614 (PCT/WO US0119142)

Priority Application: US 2000218489 20000714; US 2000642625 20000818

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 7357

Main International Patent Class: G06F-001/00

Fulltext Availability:

Detailed Description

Detailed Description

... program file is detected by a variation in the CRC value. Checksum monitors improve on integrity check systems in that it is more difficult for **malicious code** to defeat the monitoring. On the other hand, checksum monitors exhibit the same limitations as integrity checking systems in that many false warnings issue and it is difficult to identify which warnings represent actual **viruses** or infection.

Behavior **interception** systems detect **virus** activity by interacting with

the operating system of the target computer and monitoring for potentially malicious behavior. When such malicious behavior is detected, the action is blocked and the user is informed that a potentially dangerous action is about to take place. The potentially **malicious code** can be allowed to perform this action by the user. This makes the behavior **interception** system somewhat unreliable, because the effectiveness of the system depends on user input. In addition, resident behavior **interception** systems are sometimes detected and disabled by **malicious code**.

Another conventional strategy for detecting infections is the use of bait files. This strategy is typically used in combination with other **virus** detection strategies to detect an existing and active infection. This means that the **malicious code** is presently running on the target

computer and is modifying files. The virus is detected when the bait file is modified. Many viruses are aware...

33/3,K/11 (Item 7 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00862547 **Image available**

SYSTEMS, METHODS AND SOFTWARE FOR REMOTE PASSWORD AUTHENTICATION USING MULTIPLE SERVERS

SYSTEMES, PROCEDES ET LOGICIEL PERMETTANT D'AUTHENTIFIER A DISTANCE DES MOTS DE PASSE VIA DES SERVEURS MULTIPLES

Patent Applicant/Assignee:

PHOENIX TECHNOLOGIES LTD, 411 E. Plumeria Drive, San Jose, CA 95134, US,
US (Residence), US (Nationality), (For all designated states except:
US)

Patent Applicant/Inventor:

JABLON David, 7 Buckskin Drive, Westboro, MA 01581, US, US (Residence),
US (Nationality), (Designated only for: US)

Legal Representative:

NOBLES Kimberley G (agent), Irell & Manella, LLP, Suite 400, 840 Newport
Center Drive, Newport Beach, CA 92660, US,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200195545 A2-A3 20011213 (WO 0195545)

Application: WO 2001US17979 20010531 (PCT/WO US0117979)

Priority Application: US 2000209258 20000605; US 2000215835 20000703

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE
ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT
LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM
TR TT TZ UA UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 23122

Main International Patent Class: G06F-009/00

Fulltext Availability:

Detailed Description

Detailed Description

... made in the forin of a patch or update that installed by a malicious administrator, a malicious or curious hacker, or even indirectly by a **virus** . When Bob momentarily receives the value of P for a user of the system 100, the patched software can take control, **intercept** and gather these passwords, and make them available to attackers. Effectively the attacker can build his own password database, even though such a database is...

33/3,K/12 (Item 8 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00860430 **Image available**

SYSTEM AND METHOD FOR COMPREHENSIVE GENERAL GENERIC PROTECTION FOR COMPUTERS AGAINST MALICIOUS PROGRAMS THAT MAY STEAL INFORMATION AND/OR CAUSE DAMAGES

SYSTEME ET PROCEDE DE PROTECTION GENERALE COMPLETE D'ORDINATEURS CONTRE DES PROGRAMMES PERNICIEUX POUVANT VOLER DES INFORMATIONS ET/OU PROVOQUER DES DEGATS

Patent Applicant/Inventor:

MAYER Yaron, Ahad Haam Street 21, 92151 Jerusalem, IL, IL (Residence), IL (Nationality)

DECHOVICH Zak, Hasayeret Hayerushalmit 16/6, Pisgat Zeev, 97543 Jerusalem, IL, IL (Residence), IL (Nationality)

Patent and Priority Information (Country, Number, Date):

Patent: WO 200192981 A2-A3 20011206 (WO 0192981)

Application: WO 2001IL487 20010528 (PCT/WO IL0100487)

Priority Application: IL 136414 20000528; US 2000209593 20000606; US 2001284019 20010415

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR

(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG

(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW

(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 17766

Main International Patent Class: G06F-011/00

International Patent Class: G06F-013/00

Fulltext Availability:

Detailed Description

Detailed Description

... protection system preferably include.

1 .Giving the user more information about processes that would normally occur without his knowledge, thus decreasing substantially the chance that **malicious software** will be able to cheat the user.

2. Defining comprehensive yet parsimonious sets of rules of appropriate behavior of software so that the system can identify and **intercept** immediately programs that may be performing or trying to perform suspicious and/or detrimental and/or potentially dangerous activities or not behaving as usual.

3...storage media and the communication channels.

Therefore, the present invention offers the following main advantages over the prior art.

1 . It enables generic detection and **interception** of all kinds and variations of **viruses**, Trojan horses, **worms**, E-mail macro **viruses** and other vandals even when these are completely new and not similar to other vandals encountered before. Therefore, (inverted exclamation mark) it can also detect and **intercept** first strike attacks, instead of waiting for a cure after the damage has already been done to tens of millions of computers.

2. It is not dependent on constant updates of **virus** knowledge bases, unlike normal anti **virus** systems.

3. It is not dependent on inherently limited methods, such as packet filtering.

4. It offers multiple safeguards against various threats, so that a...

...updates are needed when the user downloads for example new versions or kinds of Internet applications.

7. Malicious behaviors of programs can be detected and **intercepted** even if they don't display **viral** or **worm**-like behavior at all, for example if a screen saver starts to steal data and send it out over

cominunication lines even if (inverted exclamation...

33/3,K/13 (Item 9 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00857202 **Image available**
MOBILE INFORMATION STORAGE AND COMMUNICATION DEVICE AND METHOD OF COMMUNICATION
DISPOSITIF MOBILE DE STOCKAGE ET DE COMMUNICATIONS DE DONNEES, ET PROCEDE DE COMMUNICATION

Patent Applicant/Assignee:

CYPAK AB, Svanvagen 16, S-183 77 Taby, SE, SE (Residence), SE
(Nationality), (For all designated states except: US)

Patent Applicant/Inventor:

EHRENSVARD Jacob, Svanvagen 16, S-183 77 Taby, SE, SE (Residence), SE
(Nationality), (Designated only for: US)

Legal Representative:

LENNEFORS Stefan (et al) (agent), Stockholms Patentbyra, Zacco AB, Box
23101, S-104 35 Stockholm, SE,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200190858 A1 20011129 (WO 0190858)
Application: WO 2001SE1096 20010517 (PCT/WO SE0101096)
Priority Application: US 2000574832 20000519

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ
EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR
LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL
TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Publication Language: English

Filing Language: English

Fulltext Word Count: 9370

Main International Patent Class: **G06F-001/00**

Fulltext Availability:

Detailed Description

Detailed Description

... information from a client's hard disk
without the user actually noticing that something fraudulent
is going on. A related threat is the spread of **viruses**, where
apart from direct damage, **virus** code may, from the user's per
spective, reside silent and in the background **intercept** secret
usernames, passwords and credit card numbers from user dialogues. This
information can then be processed and automati
cally transferred to an alien site. As...

33/3,K/14 (Item 10 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00766059 **Image available**
QUERY INTERFACE TO POLICY SERVER
INTERFACE D'INTERROGATION VERS SERVEUR DE REGLES

Patent Applicant/Assignee:

INTERNET DYNAMICS INC, 3717 E. Thousand Oaks Boulevard, Westlake Village,
CA 91362, US, US (Residence), US (Nationality), (For all designated
states except: US)

Patent Applicant/Inventor:

HANNEL Clifford Lee, 3178 Futura Point, Thousand Oaks, CA 91362, US, US

(Residence), US (Nationality), (Designated only for: US)
MAY Anthony Allan, 6644 Glade Avenue #217, Woodland Hills, CA 91303, US,
US (Residence), CA (Nationality), (Designated only for: US)

Legal Representative:

NELSON Gordon E, 57 Central Street, P.O. Box 782, Rowley, MA 01969, US

Patent and Priority Information (Country, Number, Date):

Patent: WO 200079434 A1 20001228 (WO 0079434)
Application: WO 2000US17078 20000621 (PCT/WO US0017078)
Priority Application: US 99140417 19990622

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AU JP SG US

(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Filing Language: English

Fulltext Word Count: 54190

Patent and Priority Information (Country, Number, Date):

Patent: ... 20001228

Main International Patent Class: G06F-017/30

Fulltext Availability:

Detailed Description

Publication Year: 2000

Detailed Description

... The IntraMap proxy is not a true proxy in that the entire connection
is always completely serviced by the instance of the IntraMap proxy that
intercepts the connection.

Anti- **Virus** Module 2033

Anti- **virus** module 2033 in a preferred embodiment is a set of DLLs
provided by Trend Micro Devices, Inc., Cupertino, CA. In other
embodiments, anti- **virus** modules from other sources may be used. Anti-
Virus module 2033 checks all data entering VPN 201 for **viruses** . In
order to provide the user with feedback on the progress of the transfer
and to prevent the user's client program from timing out...

33/3,K/15 (Item 11 from file: 349)

DIALOG(R) File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00554461 **Image available**

METHOD OF IMPROVING SECURITY IN ELECTRONIC TRANSACTIONS

PROCEDE PERMETTANT DE RENFORCER LA SECURITE DE TRANSACTIONS ELECTRONIQUES

Patent Applicant/Assignee:

INTERNATIONAL BUSINESS MACHINES CORPORATION,

ABAD PEIRO Jose L,

STOLZE Markus,

Inventor(s):

ABAD PEIRO Jose L,

STOLZE Markus,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200017834 A1 20000330 (WO 0017834)

Application: WO 99IB1494 19990902 (PCT/WO IB9901494)

Priority Application: EP 98117856 19980921

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GD GE GH
GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN
MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU
ZW GH GM KE LS MW SD SL SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY
DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML
MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 6663

Patent and Priority Information (Country, Number, Date):

Patent: ... 20000330
International Patent Class: G06F-017/60
Fulltext Availability:
Detailed Description
Publication Year: 2000

Detailed Description

... selected insurance merchant 20d'. It should be noted that even when the system appears closed, a hacker may still have been able to introduce a **virus** or a splice which can attack or **intercept** communications on either network link or 24; therefore, all intra-process communications are encrypted. Further, the machine 28 can optionally be utilized for enabling the...

33/3,K/16 (Item 12 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00537506 **Image available**

**GENERALIZED POLICY SERVER
SERVEUR DE PROCEDURE GENERALISEE**

Patent Applicant/Assignee:

INTERNET DYNAMICS INC,
HANDEL Clifford L,
LIPSTONE Laurence R,
SCHNEIDER Davis S,

Inventor(s):

HANDEL Clifford L,
LIPSTONE Laurence R,
SCHNEIDER Davis S,

Patent and Priority Information (Country, Number, Date):

Patent: WO 200000879 A2 20000106 (WO 0000879)
Application: WO 99US14585 19990628 (PCT/WO US9914585)
Priority Application: US 9891130 19980629

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AU JP SG US AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Fulltext Word Count: 35547

Patent and Priority Information (Country, Number, Date):

Patent: ... 20000106
Main International Patent Class: G06F-015/00
Fulltext Availability:
Detailed Description
Publication Year: 2000

Detailed Description

... The IntraMap proxy is not a true proxy in that the entire connection is always completely serviced by the instance of the IntraMap proxy that **intercepts** the connection.

1 5 Anti- **Virus** Module 2033

Anti- **virus** module 2033 in a preferred embodiment is a set of DLLs provided by Trend Micro Devices, Inc., Cupertino, CA. In other embodiments, anti- **virus** modules from other sources may be used. Anti- **Virus** module 2033 checks all data entering VPN 201 for viruses. In order to provide the user with feedback on the progress of the transfer and...

33/3,K/17 (Item 13 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00450528 **Image available**

**METHODS AND APPARATUS FOR CONTROLLING ACCESS TO INFORMATION
PROCEDES ET APPAREIL DE CONTROLE D'ACCES A DES INFORMATIONS**

Patent Applicant/Assignee:

INTERNET DYNAMICS INC,

Inventor(s):

JENSEN Daniel,
LIPSTONE Laurence R,
RIBET Michael B,
SCHNEIDER David S,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9840992 A2 **19980917**
Application: WO 98US4522 19980309 (PCT/WO US9804522)
Priority Application: US 9739542 19970310; US 9740262 19970310; US
9834587 19980304; US 9834503 19980304; US 9834507 19980304; US 9834576
19980304

Designated States:

(Protection type is "patent" unless otherwise stated - for applications
prior to 2004)

AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM
GW HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX
NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM
KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR
GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 38574

Patent and Priority Information (Country, Number, Date):

Patent: ... **19980917**

...International Patent Class: **G06F-001/00**

Fulltext Availability:

Detailed Description

Publication Year: **1998**

Detailed Description

... The IntraMap proxy is not a true proxy in that the entire connection
is always completely serviced by the instance of the IntraMap proxy that
intercepts the connection.

Anti- **Virus** Module 2033

Anti- **virus** module 2033 in a preferred embodiment is a set of DLLs
provided by Trend Micro Devices, Inc., Cupertino, CA. In other
embodiments, anti- **virus** modules from other sources may be used. Anti-
Virus module 2033 checks all data entering VPN 201

70

for viruses. In order to provide the user with feedback on the progress
of the transfer...

33/3,K/18 (Item 14 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00417702

ISOLATED EXECUTION LOCATION

LIEU ISOLE D'EXECUTION

Patent Applicant/Assignee:

APM LIMITED,
BULL John Albert,
OTWAY David John,
KRAMER Andre,

Inventor(s):

BULL John Albert,
OTWAY David John,
KRAMER Andre,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9808163 A1 **19980226**
Application: WO 97IB973 19970807 (PCT/WO IB9700973)

Priority Application: GB 9616783 19960809; GB 973773 19970224

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH HU
IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL
PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG US UZ VN YU ZW GH KE LS MW
SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE
IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 10377

Patent and Priority Information (Country, Number, Date):

Patent: ... 19980226

Main International Patent Class: G06F-009/46

International Patent Class: G06F-01:00

Fulltext Availability:

Detailed Description

Publication Year: 1998

Detailed Description

... be used to inspect and

verify incoming program components which it is desired to
download into the end user system and can be used to
intercept virus programs before they reach the end user
system. Whilst the end user may be confident that
specified program components are acceptable, in which case
he...

33/3,K/19 (Item 15 from file: 349)

DIALOG(R)File 349:PCT FULLTEXT

(c) 2004 WIPO/Univentio. All rts. reserv.

00388682 **Image available**

EMULATION REPAIR SYSTEM

SYSTEME DE REPARATION PAR EMULATION

Patent Applicant/Assignee:

SYMANTEC CORPORATION,

Inventor(s):

NACHENBERG Garey,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9729425 A2 19970814

Application: WO 97US1510 19970203 (PCT/WO US9701510)

Priority Application: US 96605285 19960209

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL
IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT
RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN KE LS MW SD SZ UG AM AZ BY
KG KZ MD RU TJ TM AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF
BJ CF CG CI CM GA GN ML MR NE SN TD TG

Publication Language: English

Fulltext Word Count: 8594

Patent and Priority Information (Country, Number, Date):

Patent: ... 19970814

Main International Patent Class: G06F-011/00

Fulltext Availability:

Detailed Description

Publication Year: 1997

Detailed Description

... in the virus and subroutines for restoring the host bytes to their
proper location in the host file. Such table based methods work oniv with
viruses that are identical in each instance of infection and employ
standard infection strategies. The "Thunderbyte **AntiVirus** " employs a
repair system that steps through the **viral** code, one instruction at a

time, evaluates each instruction. **intercepts** those instructions that appear likely to damage the computer system, and allows all other to execute. This system is designed to allow the **virus** ' own repair code to execute and restore the host bytes to their proper location in the host file.

New infection techniques and **virus** types have made these known repair systems increasingly unreliable. For example, once the Thunderbyte Anti-Virus system became known to virus designers, they devised ways...

33/3,K/20 (Item 16 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00360147

METHOD AND APPARATUS FOR DATA SECURITY FOR A COMPUTER
PROCEDE ET APPAREIL PERMETTANT D'ASSURER LA PROTECTION DES DONNEES D'UN
ORDINATEUR

Patent Applicant/Assignee:
ELONEX TECHNOLOGIES INC,

Inventor(s):
KIKINIS Dan,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9700472 A2 **19970103**
Application: WO 96US10280 19960614 (PCT/WO US9610280)
Priority Application: US 95490625 19950615

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

CN JP AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

Publication Language: English

Fulltext Word Count: 4901

Patent and Priority Information (Country, Number, Date):

Patent: ... **19970103**

Main International Patent Class: **G06F-000/00**

Fulltext Availability:

Detailed Description

Publication Year: **1997**

Detailed Description

... perfectly

secure. Systems may still be readily compromised by individuals, skilled in the computer arts, who are able to obtain passwords by placing smart software (**virus**) in a location on a computer, such as in its operating system, wherein the software may be operated transparent to a user. Such software may be considered a snooping routine.

Typically, snooping routines are designed to **intercept** passwords that are entered by means of a keyboard, and to store captured passwords in an address space where they may be retrieved by an...

33/3,K/21 (Item 17 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT
(c) 2004 WIPO/Univentio. All rts. reserv.

00228169 **Image available**

PROTECTION SYSTEM FOR COMPUTERS
SYSTEME DE PROTECTION POUR ORDINATEURS

Patent Applicant/Assignee:

J A S TECHNOLOGY (AUSTRALIA) PTY LTD,
WILSON Craig Stuart,

Inventor(s):

WILSON Craig Stuart,

Patent and Priority Information (Country, Number, Date):

Patent: WO 9302419 A1 **19930204**

Application: WO 92AU360 19920716 (PCT/WO AU9200360)
Priority Application: AU 917247 19910716; AU 922927 19920612

Designated States:

(Protection type is "patent" unless otherwise stated - for applications prior to 2004)

AT AU BB BG BR CA CH CS DE DK ES FI GB HU JP KP KR LK LU MG MN MW NL NO
PL RO RU SD SE US AT BE CH DE DK ES FR GB GR IT LU MC NL SE BF BJ CF CG
CI CM GA GN ML MR SN TD TG

Publication Language: English

Fulltext Word Count: 25182

Patent and Priority Information (Country, Number, Date):

Patent: ... **19930204**

Main International Patent Class: **G06F-012/14**

International Patent Class: **G06F-12:16** ...

... **G06F-12:08**

English Abstract

A system and method for protecting computer systems from computer **viruses**. The system (301) generally consists of a protection device (17) interposed between the computer and the hard disk drive (15, 307). The protection device (17) is connected between the disk controller (13, 303) and the disk drive (15, 307) to **intercept** relevant control signals issued by the controller (13, 303) to the disk drive (15, 307) and selectively override the signals in accordance with a prescribed...